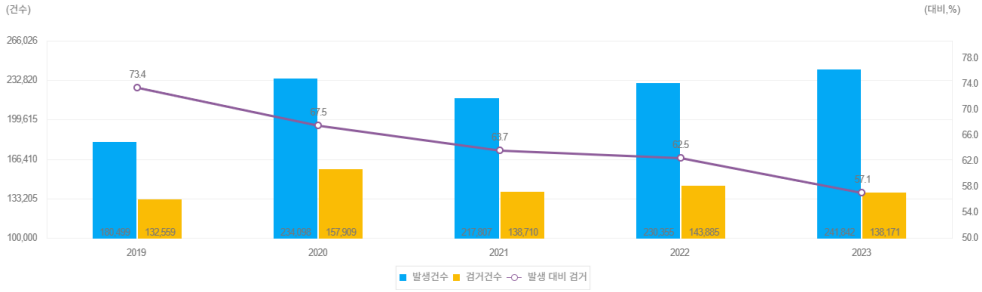
5월 국외 교육 동향 발행일 : 2025년 5월 21일 발행처: 경상북도교육청연구원

딥페이크 등 디지털 범죄 예방 교육

Education on Deepfakes and Digital Crime Prevention

디지털 범죄의 발생과 예방 교육의 필요성



자료를 보면 과거에 비해 우리나라의 디지털 범죄 발생 건수 자체가 증가하는 것을 확인할 수 있다. 더욱 주목해야할 부분은 **발생 대비 검거 비율이 점차 감소**하고 있다는 것이다. 디지털 범죄의 특성상 가해자를 특정하고 찾기가 어려운 만큼, **교육을 통한 디지털 범죄의 예방이 무엇보다 중요하다.**

[자료 출처: e-나라지표]

디지털 범죄 예방 교육의 확산

디지털 환경이 확대되면서 청소년들은 디지털 괴롭힘, 유해 콘텐츠 노출, 개인정보 유출 등 다양한 디지털 위험에 노출되고 있다. 이러한 위험에 대비해 **세계 각국은 학교 교육에서 디지털 시민성과 디지털 윤리 교육을 강화하는 추세이다.** '유네스코'는 디지털 시민성 교육 지침을 통해 미디어 리터러시 및 디지털 윤리 교육을 제공하여 학생들이 디지털 공동체에 건설적으로 참여할 수 있도록 지원하고 있다.

[자료 출처: OECD edutoday, UNESCO]

디지털 범죄 예방 교육의 의미

예방 교육은 단순히 범죄로부터의 보호를 넘어, 학생들이 디지털 환경 속에서 책임감 있고 안전하게 행동할 수 있는 주체적 시민성을 함양하는 데 목적을 둔다. 특히 사이버 괴롭힘, 개인정보 침해, 온라인 금융 사기 등 구체적 사례를 중심으로 상황 대응 능력을 기르는 교육이 확산되고 있으며, 이는 **학생 개인뿐 아니라 건강한 디지털 공동체를 구축하는 데 필수적인 기반으로 여겨지고 있다.**

독일

▸ 독일에서의 디지털 범죄 예방 교육 기반

- 미디어 리터러시 교육을 의무적으로 시행
- 딥페이크를 비롯한 디지털 범죄 예방 노력

▸ 디지털 범죄 예방 교육 사례(노르트라인베스트팔렌주)

- **주제:** 사이버 그루밍 예방
- **대상:** 3~6학년(초등학교, 중학교)
- **내용:** 인터넷 ABC가 어린이를 사이버 성폭력으로부터 보호하는 데 도움을 주기 위해 개발함.

- **주제:** 데이터 보호
- **대상:** 3~6학년(초등학교, 중학교)
- **내용:** 연방 시민교육청이 제공하는 서비스로 데이터 보호법, 데이터 보호 책임자의 역할, 아동과 청소년의 권리 등에 대해 알려줌.

- **주제:** 디지털 시대의 가짜 뉴스와 소셜 미디어
- **대상:** 10~11학년(고등학교)
- **내용:** 인터넷상의 잘못된 정보, 조작, 여론 형성에 대한 인식을 높이고, 자신의 미디어 사용에 대해 반성하고, 온라인 문화를 적극적으로 형성 하는데 초점이 맞춰짐.

- **주제:** 일상생활 속 미디어 발견과 이해
- **대상:** 유치원 이상
- **내용:** 어린이가 일상생활에서 놀이 중심으로 미디어를 능숙하게 사용할 수 있도록 방법을 제시함.

- **주제:** 알고리즘은 소셜 미디어에서 어떤 역할을 하는가?
- **대상:** 5~13학년(중학교, 고등학교)
- **내용:** Instagram, TikTok, YouTube 같은 소셜 미디어에서 알고리즘은 필요한지, 알고리즘에 대한 의견 표명하기 등

핀란드

핀란드는 점점 정교해지는 디지털 범죄 양상에 대응하기 위해 디지털 범죄 예방 및 해결 과정 전체를 포괄하는 **다층적 안전망을 마련해 학생들을 보호하고 있다.** 여기에는 학생뿐 아니라 학교, 교사, 학부모, 지역사회, 경찰, 민간단체 등 모든 주체가 함께 책임을 나누고 협력한다.

▸ 교육과정 및 정책

미디어 리터러시 교육의 강조를 통한 디지털 범죄 대처 역량 강화

▸ 학교와 교육 현장

여러 과목과 비교과 활동 등 교육의 전 방면에서 디지털 범죄 예방 교육 실행

▸ 지역사회

경찰, 시민 단체 등 지역 사회가 주도하는 다양한 캠페인 활동 실시

영국

디지털 범죄 예방 **[딥페이크 : 새로운 위협의 부상]**

▸ 교육적 통합

디지털 리터러시, 컴퓨팅 교육

- 온라인 안전과 책임있는 디지털 시민의식 함양

▸ 다원적 노력

정책적, 기술적 대응 및 교직원 연수

- 피해자 지원, 콘텐츠 필터링, 신종 온라인 위협 이해

▸ 외부 협력

NCA, NCSC, UKSIC, IWF 등

- Cyber choices 프로그램 제공
- Safer Internet Day 캠페인

▸관련 법규

Online Safety Act (2023)

- 온라인 유해 콘텐츠 차단
- 플랫폼 운영 책임 강화

프랑스

사이버 괴롭힘은 정신 건강, 학업 성취, 사회성 발달에 부정적인 영향을 미치는 주요 교육 문제로 부상했다. 프랑스 교육부는 법적 대응 강화, 부처 간 협력 체계 구축, pHARe 프로그램의 전국적 의무 시행 등을 통해 문제에 체계적으로 대응하려는 의지를 보여주고 있다. pHARe 프로그램은 예방 교육, 보호 공동체 형성, 효과적 개입, 학부모 및 파트너 참여, 학생 주도 활동 등 다각적인 접근을 특징으로 한다. 또한, 3018 전용 상담 전화와 같은 지원 시스템 운영과 디지털 시민성 교육 강화 역시 중요한 정책 요소로 포함된다. 그러나 이러한 노력에도 불구하고 여러 과제가 남아 있다. 정책의 효과성에 대한 독립적이고 엄밀한 평가가 부족하며, 현장에서는 교직원 교육과 자원의 부족, 지역 및 학교 간 실행 편차, 끊임없이 변화하는 디지털 환경에 대한 적응 문제 등이 지적된다. 이를 극복하기 위한 정책적 보완이 과제로 남아 있다.

▸ 디지털 폭력에 대한 프랑스의 인식, 대응, 교육 정책

가중 처벌 조항

가중 처벌 조항은 디지털 폭력에 대한 강력한 대응을 시사함

pHARe 프로그램

pHARe 프로그램은 디지털 폭력에 대한 온, 오프라인에서의 대응이 가능하도록 도움

기관 간 협력

공공 기관, 시민 단체, 기업 등의 인적 물적 지원, 협력, 교육 활동 참여

3018 상담 전화 운용

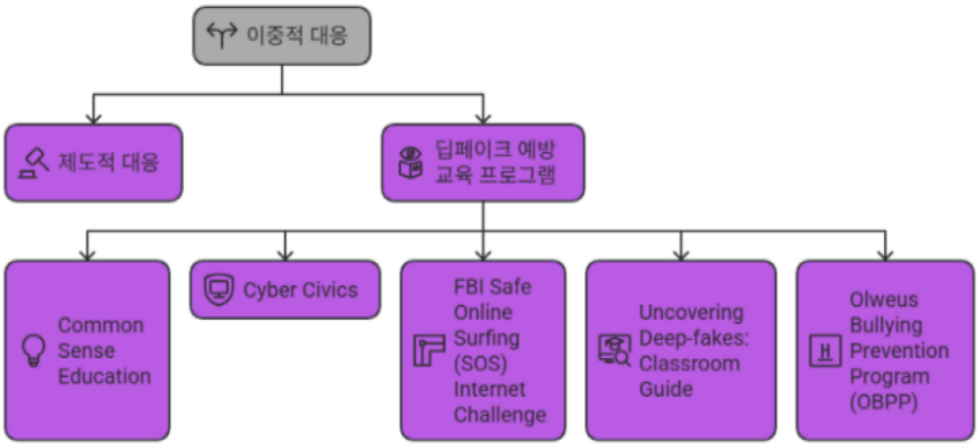
피해 학생과 가족에 대한 세밀하고 구체적인 지원을 목적으로 운용

미국

▸ 딥페이크 예방 교육 프로그램

· 이중적 대응

1. 제도적 대응: Title IX 규정 개정
2. 딥페이크 예방 교육 프로그램 : Common Sense Education, Cyber Civics, FBI Safe Online Surfing (SOS) Internet Challenge, Uncovering Deep-fakes: Classroom Guide, Olweus Bullying Prevention Program (OBPP)

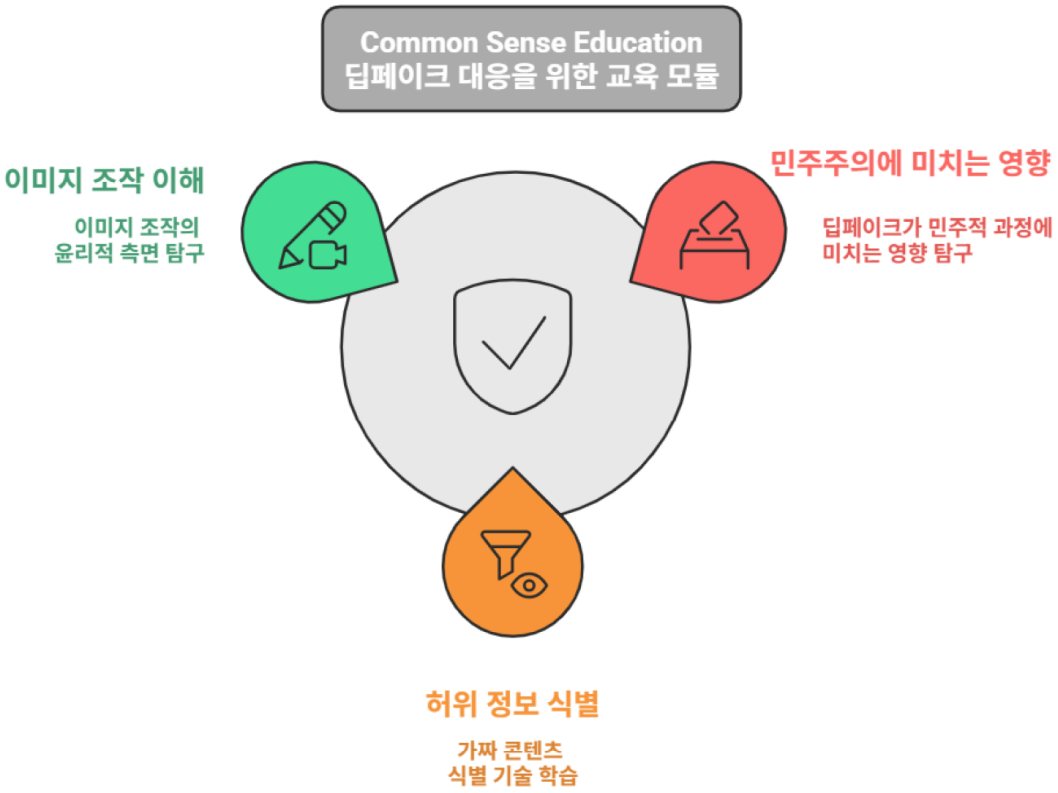


▸ AI for Education: 딥페이크의 다면적 탐구

1. 비동의 딥페이크 이미지
2. 청소년 대상 딥페이크 범죄
3. 권위자 사칭
4. 딥페이크의 사회적 영향
5. 딥페이크의 규제 필요성
6. 딥페이크의 긍정적 활용

▸ Common Sense Education 딥페이크 대응을 위한 교육 모듈

1. 이미지 조작 이해
2. 민주주의에 미치는 영향
3. 허위 정보 식별

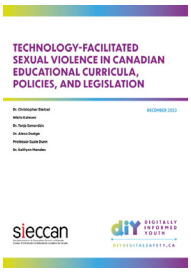


캐나다

▸ 배경 및 실태

- 캐나다인의 60% 이상이 딥페이크 이미지, 비디오 경험
- 여성, 장애인, 이주 배경, 성소수자 등 소수자 청소년의 딥페이크 성범죄 피해 확률 ↑
- 미성년자 성적 사진은 딥페이크 여부와 상관없이 아동 음란물로 처벌, Cybertip.ca (미성년 온라인 성 착취 국가 직통 신고 창구) 운영

▸ 캐나다의 청소년 디지털 성범죄 연구기구, DIY



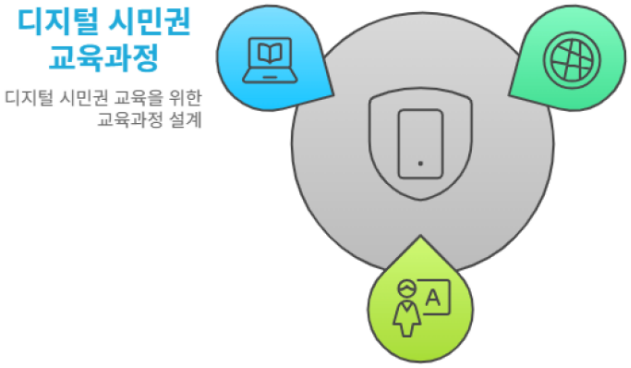
- 디지털 안전 연구 프로젝트(Digital Safety research project)를 통해 캐나다 전역 주/준주별 교육부의 디지털 성범죄 대처 분석
- 디지털 성범죄 관련 주/준주별 교육과정 및 교육 정책 평가
- 교육과정 및 교육 정책 개선 방향 제시

▸ 주/준주 교육계별 디지털 성범죄 대응 노력

- 브리티시 컬럼비아 주: 교육과정에 건강한 관계, 기술 윤리, 디지털 시민성 등 포함
- 온타리오 주: 보건, 컴퓨터 과목 이용해 관계, 의사소통, 안전한 기술 사용, 윤리 등 지도
- 퀘벡 주: 성교육, 윤리 과목에서 관계 내 폭력, 사이버 괴롭힘 중심으로 비판적 사고, 책임감 함양

호주와 뉴질랜드

▸ 호주의 디지털 범죄 예방 교육



디지털 시민권 교육과정

디지털 시민권 교육을 위한 교육과정 설계

국가적 노력

강력한 법률과 제도를 통해 모든 시민을 보호하기 위한 정부의 광범위한 노력

교육적 지원

학교와 교사를 위한 방대한 교육자료 제공

▸ 뉴질랜드의 디지털 범죄 예방 교육

Kete

학교 온라인 안전교육 지원

AI and online safety

디지털 범죄에 대한 대응 강화

Netsafe

디지털 범죄 예방 교육 및 컨설팅 제공

IWF

유해 사이트 차단 및 삭제

일본

▸ 일본의 딥페이크 예방 교육 사례

방 법	내 용	모 습
법적 대응 방안	· 일본의 형법, 개인정보보호법, 명예훼손에 관한 법률을 중심으로 딥페이크 제작 및 유포가 법적 처벌 대상임을 설명함. · 학교에서는 경찰청과 협력해 정기적으로 강연을 진행함으로써 학생들이 법적 지식을 접할 수 있는 기회를 제공하고 있음.	
역할극	· 학생들은 가상의 상황을 설정하고 딥페이크 피해자가 되었을 때의 대처 방법을 고민하며 해결책을 모색함. · 이러한 역할극을 통해 학생들은 딥페이크 관련 피해 발생 시 신속하게 대응할 수 있는 능력을 갖추게 되며, 딥페이크 영상의 제작 및 유포가 타인에게 심각한 피해를 줄 수 있음을 인식하게 됨.	
프로젝트 학습	· 학생들은 직접 인터넷에서 가짜 뉴스 사례를 분석하거나 AI 기술을 활용해 영상이 조작되었는지 판별하는 프로그램을 체험하면서 생성형 AI 기술에 대한 이해도를 높임. · 이러한 교육은 학생들이 딥페이크의 위험성을 이론적으로 배우는 것을 넘어 실생활에 직접 적용하고 일상 속 피해를 예방하는 힘을 기르는데 도움이 됨.	
인터뷰 체험 게임	· 미디어 리터러시 교육의 일환으로 학생들이 각자 기자가 되어 다른 학생들의 인터뷰를 진행함. · 면접 과정에서 다른 학생들의 대답 속 상충되는 부분 등을 토대로 거짓 정보를 식별하는 연습을 게임 형태로 실시함	

기획 및 편집	경상북도교육청연구원 정책연구부 교육연구사 안주연 및 발간위원 8명		
표지 디자인	이천초등학교 교사 최휘도	**주소**	054-840-2276
주소	경상북도 안동시 강남로 152	**WEB**	www.gbe.kr/gber

딥페이크 등 디지털 범죄 예방 교육

Education on Deepfakes and Digital Crime Prevention

독일의 딥페이크 등 디지털 범죄 예방 교육

발간위원 : 최신영 (영주가흥초등학교 교사)

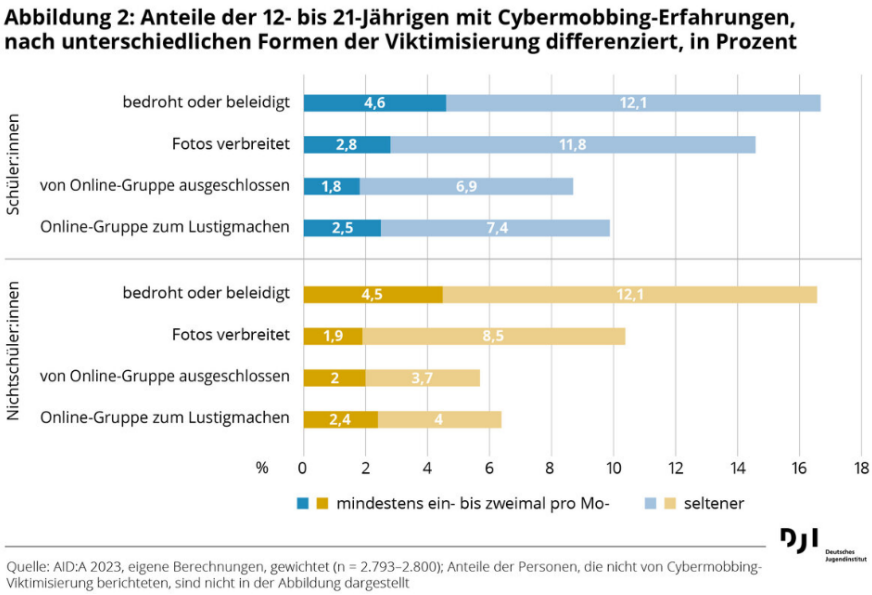
디지털화된 학생의 일상은 여러 측면에서 다양한 기회를 제공받는 동시에 위험이 따른다. 일상생활에서 사이버 괴롭힘을 당하는 학생의 비율이 늘어나고 있다. 사이버 괴롭힘은 전문가뿐만 아니라 피해를 본 청소년과 그 가족들 사이에서도 많이 논의되는 위험 중 하나이다.

이라 카타리나 페터와 프란츠 페터만(Ira-Katharina Peter und Franz Petermann, 2018)의 정의에 따르면, 사이버 괴롭힘은 정보 및 통신 기술을 사용하여 다른 사람을 반복적·고의로 괴롭히거나 당황하게 만드는 것이다. 사이버 괴롭힘은 소셜 미디어, 메신저 서비스, 이메일, 채팅 등 다양한 수단을 통해 발생할 수 있다. 사이버 괴롭힘 피해는 심각한 심리적·신체적·사회적 문제를 초래할 수 있다.

독일 청소년 연구소(Deutsches Jugendinstitut, DJI)가 실시한 조사 결과, 12~21세 청소년의 약 7%가 지난 몇 달 동안 사이버 괴롭힘을 경험했다고 응답했다(응답자가 한 달에 한두 번 이상 하나 이상의 손해를 입었다고 한 경우, 사이버 괴롭힘을 경험한 것으로 간주함). 사이버 괴롭힘의 유형은 다음과 같다.

- ◆ 누가 나를 놀리는 온라인 그룹을 만들었다(약 2%).
- ◆ 아무 이유 없이 온라인 그룹에서 추방당해서 기분이 나빴다(약 2%).
- ◆ 내 동의 없이 내 부끄러운 사진이나 그림이 유포되었다(약 2%).
- ◆ 스마트폰이나 인터넷을 통해 위협이나 모욕을 당한 적이 있다(약 5%).

또한 이 조사는 학교에 다니지 않는 학생과 청소년도 사이버 괴롭힘 피해의 네 가지 유형 관련해 통계적 측면에서 차이가 없다고 밝혔다(그림 1).



[그림 1] 사이버 괴롭힘 조사 결과(DJI)

12~21세 청소년 중 67%는 사이버 괴롭힘을 당한 적이 있다고 보고했다. 이 조사 결과는 사이버 괴롭힘이 학생들에게만 문제가 되는 게 아니라, 학교 환경 밖에서도 훈련, 학업, 취업 면에서도 영향을 받는다는 사실을 분명히 보여준다. 학교뿐만 아니라 인터넷과 소셜 미디어 자체에서 예방 프로그램이 필요함을 나타낸다.

1. 미디어 역량 프레임워크(Medienkompetenzrahmen)

미디어 역량 프레임워크는 독일 내 모든 초등학교와 중학교에서 미디어 리터러시 역량을 기르고, 직업대학에서 디지털 핵심 기술을 증진하기 위한 학교 및 교육 개발 표준이다. 디지털 변화가 제공하는 기회에 모든 어린이와 청소년이 참여할 수 있도록, 미디어를 안전하고 창의적이며 책임감 있게 사용할 수 있도록 돕고, 기본적인 정보 기술 능력과 포괄적인 미디어 역량을 기르는 것을 목표로 한다.

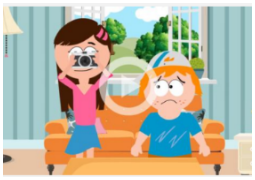
이러한 배경하에, 독일연방공화국의 각 주 교육부와 문화부 장관 상임 회의는 2016년 12월 '디지털 세계의 교육(Bildung in der digitalen Welt)' 전략을 채택했으며, 이 전략에서 모든 주는 미디어를 다루기 위한 공통 역량 프레임워크에 합의했다. 연방주는 2018/2019학년도에 초등학교, 중학교에 입학하는 모든 학생이 의무 교육을 마치기 전까지 이 프레임워크에 규정된 기술을 습득할 수 있도록 하였다.

가. 미디어 리터러시 프레임워크 NRW(노르트라인베스트팔렌주)

노르트라인베스트팔렌주에서는 안전하고 창의적이며 책임감 있는 미디어 사용을 위해 '미디어 리

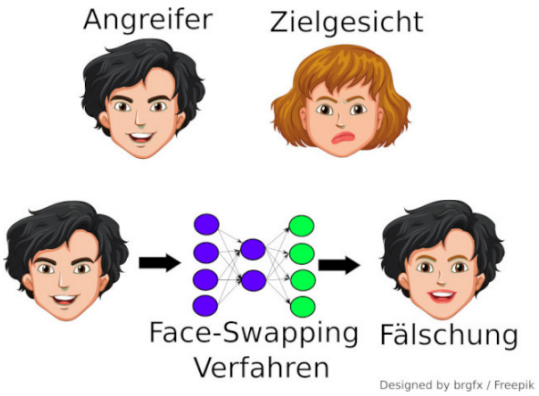
터러시 프레임워크 NRW'에 다음의 역량을 제시하였다.

〈표 1〉 미디어 리터러시 프레임워크 NRW의 역량과 수업 자료 예시

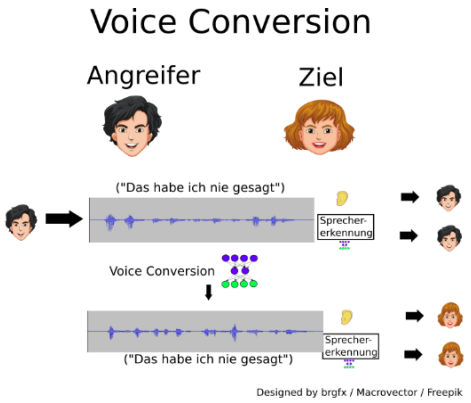
역량	수업 자료 예시	
작동과 응용		-주제: 사이버 그루밍 예방 -대상: 3~6학년(초등학교, 중학교) -내용: 인터넷 ABC가 어린이를 사이버 성폭력으로부터 보호하는 데 도움을 주기 위해 개발함.
		-주제: 데이터 보호 -대상: 3~6학년(초등학교, 중학교) -내용: 연방 시민교육청이 제공하는 서비스로 데이터 보호법, 데이터 보호 책임자의 역할, 아동과 청소년의 권리 등에 대해 알려줌.
알림 조사 분석 반성		-주제: 디지털 시대의 가짜 뉴스와 소셜 미디어 -대상: 10~11학년(고등학교) -내용: 인터넷상의 잘못된 정보, 조작, 여론 형성에 대한 인식을 높이며, 자신의 미디어 사용에 대해 반성하고, 온라인 문화를 적극적으로 형성하는데 초점이 맞춰짐.
소통과 협력		-주제: 일상생활 속 미디어 발견과 이해 -대상: 유치원 이상 -내용: 어린이가 일상생활에서 놀이 중심으로 미디어를 능숙하게 사용할 수 있도록 방법을 제시함.
제작 및 발표		-주제: 지식 재산권 보호 -대상: 1~5학년(초등학교, 중학교) -내용: 이야기를 중심으로 지식 재산권 보호의 기본을 알려줌.
문제 해결 및 모델링		-주제: 알고리즘은 사악하거나 위험한가? -대상: 5~13학년(중학교, 고등학교) -내용: 알고리즘이 실제로 좋은지 나쁜지, 알고리즘을 훈련하기 위해 무엇을 할 수 있는지 알아봄.
		-주제: 알고리즘은 소셜 미디어에서 어떤 역할을 하는가? -대상: 5~13학년(중학교, 고등학교) -내용: Instagram, TikTok, YouTube 같은 소셜 미디어에서 알고리즘은 필요한지, 알고리즘에 대한 의견 표명하기 등

2. 딥페이크 – 위험과 보호

미디어 정체성을 조작하는 방법은 수년간 존재해 왔다. 다양한 방법을 사용하여 이미지 조작이 가능함은 널리 알려져 있다. 오랫동안 비디오나 오디오 녹음과 같은 동적인 미디어를 고품질로 조작하기는 매우 어려웠으나 인공지능(AI)으로 인해 조작이 훨씬 쉬워졌으며 비교적 적은 노력과 전문 지식으로 고품질의 위조품을 만들 수 있다. 따라서 독일 연방정보기술보안청(Bundesamt Fur Sicherheit in der Informationstechnik, BSI)에서는 미디어 정체성을 조작하는 방법을 세 가지 미디어 형태(비디오/이미지, 오디오, 텍스트)로 나누어 제시하였다(그림 2, 그림 3).



[그림 2] 얼굴 조작



[그림 3] 목소리 조작

미디어 정체성 조작 가능성으로 인해 수많은 위협 시나리오가 생겼다. BIS에서는 위협 시나리오로 네 가지를 들었다.

- **생체 인식 시스템 극복:** 딥페이크 기술을 이용하면 대상 인물의 특징을 담은 미디어 콘텐츠를 제작할 수 있고, 생체 인식 시스템에 큰 위험이 됨.
- **사회 공학:** 딥페이크 기술은 정보와 데이터를 얻기 위해 특정 대상을 겨냥한 피싱 공격을 수행하는 데 사용될 수 있음.
- **허위 정보 유포:** 주요 인물이 조작한 미디어 콘텐츠를 제작하고 배포하여 신뢰할 만한 허위 정보 유포 가능성이 높음.
- **명예훼손:** 허위사실 유포로 개인의 명예가 영구적으로 손상될 수 있음.

독일은 아직 합법적인 딥페이크와 범죄 딥페이크를 구분하는 별도의 법률이 없다. 하지만 기존의 권리와 법률은 이미 시민을 딥페이크의 임의적인 오용으로부터 보호하고 있다.

- 기본법 제1조: 인간 존엄성의 보호
- 형법 제201조 a항: 자기 초상에 대한 권리
- 형법 제184조의 2: 아동 음란물의 배포, 취득 및 소지

◆ 형법 제185조: 모욕죄 ◆ 형법 제187조: 명예훼손 ◆ 저작권법 제97조: 삭제권
◆ 네트워크 시행법(NetzDG) ◆ 일반 데이터 보호 규정(GDPR)

3. 학교에서의 미디어 리터러시 교육 사례

가. 8~13학년 대상 미디어 리터러시 교육(바덴뷔르템베르크주)

2019/2020학년도부터 모든 과목에 '민주주의 교육 지침'을 제시하였는데, 여기에 미디어에 관한 내용이 담겨 있다. 학생은 미디어에 대한 지식을 습득하고, 이를 비판적으로 활용·형성하는 방법을 배우며, 자신의 미디어 행동과 미디어 시스템을 성찰해 봐야 한다. 9학년부터는 지각 능력과 현실과 허구를 구별하는 법을 훈련하는 게 중요하다. 가짜 뉴스와 영화 속임수가 한 가지 주제가 될 수도 있다. 수업은 사용하는 자료에 따라 4~10시간 정도 소요되며, 각 모듈은 개별적으로 가르칠 수 있으나 모듈 1~3의 순서를 유지하는 게 합리적이다.

〈표 2〉 8~13학년 대상 미디어 리터러시 교육

단계	내용
모듈 1: 가짜 뉴스 인식	가짜 뉴스를 알아차리는 것은 쉽지 않으며, 보도가 너무 많아서 지칠 수 있다. 학생들은 가짜 뉴스를 감지하는 도구를 배워야 하는데, 이때 학생들이 내용을 잘 알 수 있도록 최신 주제를 다루는 것이 필수이다. 텍스트를 읽고 내용을 요약한 후 독자는 왜 텍스트가 '가짜'로 인식될 수 있는지 알아야 한다.
모듈 2: 딥페이크	학생들에게 두 장의 사진이 제시되는데 학생들은 그 사진을 보고, 무슨 일이 있었는지 설명해야 한다. 딥페이크 관련 영상 시청 후 교실 토론을 하고, 소그룹으로 나누어 보호 방법에 대해 논의한다.
모듈 3: 가짜로서의 영화	수업에 적합한 영화를 감상한다. 이 영화를 처음 볼 때는 반드시 속임수라고 의심하지 않으나, 이 영화는 속임수를 사용한다. 영화에 이어 조작적으로 사용된 기술이 소개된다. 영화를 통해 이미지와 영화가 반드시 현실을 반영하는 것은 아니며, 사람은 쉽게 조종될 수 있다는 것을 보여준다.

나. 8~13학년 대상 미디어 리터러시 교육(바덴뷔르템베르크주)

바덴뷔르템베르크 주립 미디어 센터(LMZ)가 제공하는 미디어 교육 프로그램 'Bitte Was? Countering Fake and Hate'와 같은 청소년 미디어 보호 프로젝트를 통해 학생들은 허위 보도를 식별하는 법을 배우고 인터넷의 위험성을 인식할 수 있다.

RESPEKTBW 프로젝트는 인터넷상의 증오, 가짜 뉴스, 선동에 대한 명확한 메시지를 보내고자 기획되었다. 학생들이 온라인에서 성찰적이고 긍정적인 방식으로 상호작용 하도록 동기를 부여하려

면 학생의 삶과 직접 관련된 현대적인 제안이 필요하다. 따라서 4가지 접근 방식을 제시하고 있다.

- ◆ **창의적 경쟁- SETZEN 챌린지:** 학교, 교육기관, 학생들은 다양성과 관용을 옹호하고 증오, 선동, 허위 정보에 맞서기 위해 자신만의 창의적인 기여 작품을 디자인하고 제출해야 함.
- ◆ **정보 및 인식 캠페인:** 도전을 지원하는 것 외에도, 가짜 뉴스와 인터넷상의 증오에 대한 흥미로운 정보와 영상이 캠페인 채널을 통해 공유됨.
- ◆ **교육자료 및 훈련:** 교실에서 지속적인 과제를 수행하기 위해 교사들에게 다양한 지원 자료가 제공됨.
- ◆ **이벤트 및 워크숍:** 캠페인과 함께 주 전역에서 무료 이벤트와 워크숍이 진행됨.

4. 맺음말

독일에서는 미디어 리터러시 교육을 의무적으로 시행하여 딥페이크를 비롯한 디지털 범죄 예방에 힘쓰고 있다. AI 활용 범죄의 심각성을 인식하고 다양한 해결 및 예방 방법을 모색하여 적극적으로 대응하고 있다.

【참고 자료】

- ▸Deepfakes – Gefahren und Gegenmaßnahmen https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Kuenstliche-Intelligenz/Deepfakes/deepfakes_node.html
- ▸Fakes in den Medien, https://www.schule-bw.de/faecher-und-schularten/sprachen-und-literatur/deutsch/unterrichtseinheiten/fake-news
- ▸Medienkompetenzrahmen NRW,https://www.schulministerium.nrw/medienkompetenzrahmen-nrw
- ▸Medienkompetenz rahmen NRW, https://medienkompetenzrahmen.nrw/
- ▸Mobbing im Internet, https://www.dji.de/themen/kinderschutz/cybermobbing.html
- ▸RespektBW: BITTE WAS?! Kontern gegen Fake und Hass, https://www.lmz-bw.de/angebote/alle-angebote/bitte-was-kontern-gegen-fake-und-hass
- ▸Sind Deepfakes in Deutschland legal?, https://www.lmz-bw.de/lmz-spotlights/deepfakes-tipps-fuer-eltern-und-lehrkraefte

핀란드의 딥페이크 등 디지털 범죄 예방 교육

발간위원 : 최희도 (아천초등학교 교사)

디지털 환경은 학습의 경계를 넓혔지만 동시에 새로운 위험을 함께 안겨주었다. 사이버 괴롭힘, 디지털 성범죄, 딥페이크와 같은 문제는 이제 교육이 외면할 수 없는 현실이 되었다. 핀란드는 이러한 변화 속에서 교육의 역할을 새롭게 정의하고 있으며 기술을 가르치는 것을 넘어 디지털 환경에서 안전하고 책임감 있게 살아갈 수 있는 역량을 학생들에게 길러주고자 한다.

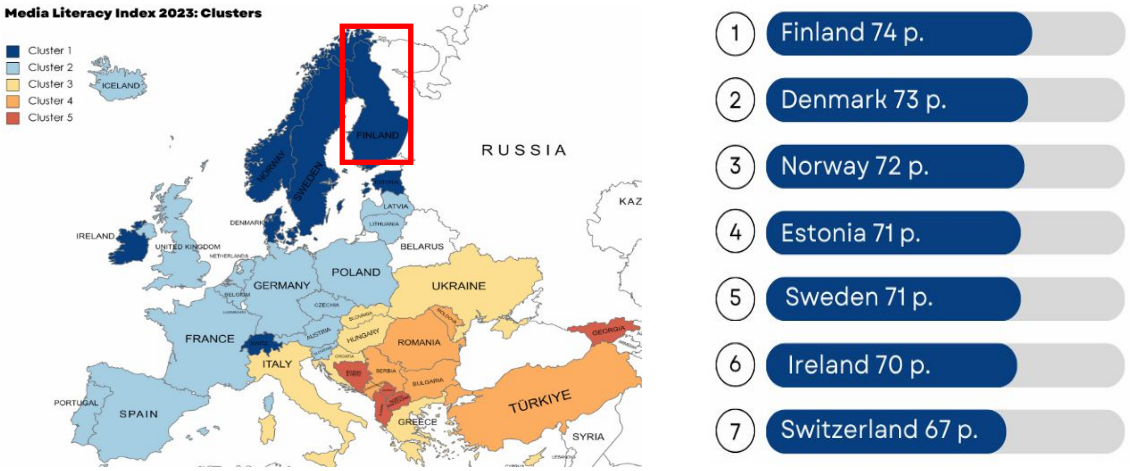
1. 핀란드의 청소년 대상 디지털 범죄

핀란드에서 청소년 대상 디지털 범죄 문제는 다른 나라들과 마찬가지로 중요한 사회적 해결 과제로 인식되고 있다. 최근 조사에 따르면 핀란드 청소년의 약 12%가 사이버 괴롭힘 피해를 당해본 적이 있고 8%가 가해 행위를 한 경험이 있는 것으로 보고되었다. 또한 많은 핀란드 학생들이 온라인에서 괴롭힘, 따돌림, 모욕을 경험하거나 보았으며, 특히 성적인 모욕과 외모적인 비하가 학생들에게 큰 상처를 주는 것으로 파악되었다.[1] 함께 온라인에서 이뤄지는 성인의 부적절한 접근과 성적 메시지도 심각한 문제로 대두되고 있다. 한 설문에서는 11~17세 사이의 응답자 1,762명 중 약 62%가 자신보다 연장자인 성인으로부터 온라인 연락을 받은 적이 있다고 답변했고, 17%는 매주, 29%는 적어도 매월 한 번 이상 성인으로부터 성적인 내용이 담긴 메시지를 받는다고 응답했다. 특히 여학생의 92%는 한 번 이상 이러한 성적 메시지를 받아본 적이 있다고 응답하여 디지털 성범죄 위험성 매우 심각하다는 것을 보여주었다.[2] 딥페이크와 같은 신종 디지털 기술을 악용한 허위 정보 사용 및 성범죄 사례도 증가하는 추세에 있어, **핀란드 사회 내에서도 청소년을 보호하기 위한 선제적 디지털 범죄 예방 교육 중요성이 점차 커지고 있다.**

1) https://www.samha.fi/en/cyberbullying/
2) https://www.inhope.org/EN/articles/save-the-children-finland-publish-report-on-online-grooming

2. 국가 정책을 통한 디지털 범죄 예방

핀란드 정부는 이러한 디지털 범죄로부터 아동과 청소년을 보호하기 위해 국가 정책과 교육과정 차원에서 종합적인 대책을 추진하고 있다. 특히 **'미디어 리터러시' 교육을 일찍부터 강조하여 디지털 환경에서의 학생들이 위험을 파악하고 대처할 수 있도록 노력해 왔다.** 실제로 2013년에 핀란드는 유럽에서 가장 먼저 미디어 리터러시를 국가 교육정책으로 공식 도입하였으며, 2019년부터는 유아기부터 고등학교에 이르기까지 모든 교과과정에 미디어 리터러시를 지도하고 있다. 이렇듯 핀란드 학생들은 다양한 교과 수업 속에서 디지털 자료를 비판적으로 바라보고 디지털 공간의 위험을 파악하는 법을 배우고 있는 것이다. 일례로 핀란드 초등학교에서는 뉴스가 어디에서 왔는지 출처를 확인하고, 온라인에서 이뤄지는 표현의 자유와 책임에 대해 알아보는 '가짜뉴스 파악하기 학습'이 이뤄지고 있다. 이러한 노력 덕분에 핀란드는 미디어 리터러시 지표에서 꾸준히 유럽 1위를 차지하며, 디지털 범죄 예방을 위한 결실을 거두고 있다.



[그림 1] 2023 미디어 리터러시 지표 (The Media Literacy Index 2023)[1)]

3. 교육 현장에서의 디지털 예방 교육

핀란드의 학교 현장에서는 교과 및 비교과 활동을 통해 일상적으로 디지털 범죄 예방 교육이 이뤄지고 있다. 예를 들어 보건 수업 시간에 디지털 성범죄 사례를 확인하고 디지털 성범죄 예방 교육을 진행하거나, 사회 수업에서 사이버 괴롭힘이 미치는 영향과 법적 책임을 다루는 등 ICT 활용 수업 및 사회, 생물, 보건 과목 등을 통해 디지털 안전, 개인정보 보호, 성적 자기결정권 등을 가르치고 있다. 또한 앞서 밝힌 것처럼 모든 교과에서 미디어 리터러시를 강조하여 학생들이 자연스럽게 딥페이크 영상이나 허위정보를 판별하는 방법을 익힐 수 있도록 노력하고 있다. 이렇듯 **핀란드에서 디지털 예방 교육은 독립된 한 과목이 아니라 여러 과목에 걸쳐 통합적으로 지도되고 있으며 학생이 문제 상황을 만났을 때 스스로 대처하고 선택할 수 있도록 지원하고 있다.**

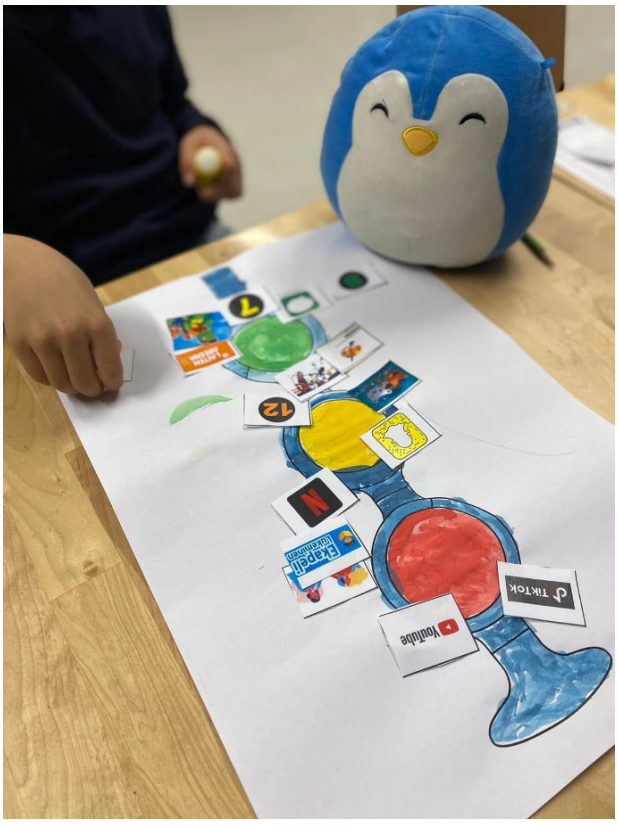
1) https://osis.bg/wp-content/uploads/2023/06/MLI-report-in-English-22.06.pdf

가. 키바(KiVa) 프로그램

비교과 활동과 학교 특색 프로그램을 통해서도 디지털 범죄 예방 교육은 활발히 이뤄지고 있다. 핀란드의 대표적인 **학교폭력 예방 프로그램인 '키바(KiVa)'는 오프라인 학교폭력뿐만 아니라 온라인 학교폭력까지 포괄한다.** 2009년 핀란드 교육문화부의 지원으로 개발된 키바 프로그램은 현재 핀란드 종합학교의 90% 이상에서 도입되어 유의미한 효과를 거두고 있다. 키바 프로그램은 존중, 감정 조절 등 디지털 학교 폭력 예방 교육과, 문제 개입 절차 과정 그리고 사후 관리 모니터링 과정으로 구성되어 있다. 이를 통해 학교 구성원 모두가 디지털 학교 폭력 문제를 인식하고 역할을 분담하며 대응할 수 있도록 노력한다. 각 학교에는 전문 훈련을 받은 3명의 교사로 구성된 전담팀이 있다. 키바 전담팀에서는 사안이 발생하면 피해 학생 면담, 가해 학생 지도 및 행동 수정, 관련 학생 추가 면담을 진행하고 필요한 경우 학부모 및 관련기관과 연계한다. 이처럼 핀란드는 디지털 학교 폭력 범죄에 대한 학교 차원의 표준 대응 절차를 마련함으로써 디지털 문제도 학교폭력의 연장선으로 인식하고 해결하고 있는 것이다.

나. Stop, Slow & Go 프로그램

저연령 학생들을 위한 프로그램도 진행되고 있다. 유아 및 초등학교 즉, 디지털 세계를 처음 접하는 단계에서부터 올바른 습관을 익히고 위기 상황에 대처하는 방법을 가르치고 있는 것이다. **'Stop, Slow & Go 프로그램'은 빠르게 변화하는 디지털 환경에서 아이들이 어떻게 반응해야 할지 놀이와 이야기를 통해 학습**하는 교육 프로그램으로서, 학생들이 위험한 온라인 상황에서 **'일단 멈추고 신중히 생각한 후 안전하면 진행한다'**라는 의사결정 능력을 키우도록 돕는다. 이 프로그램은 교사와 부모가 함께 활용할 수 있도록 워크숍 형태로 제공되며 학생들이 겪은 디지털 경험을 어른들과 공유하도록 권장한다. 이러한 교육을 통해 핀란드의 학생들은 상대적으로 어린 시기부터 디지털 범죄로부터 자신을 보호하는 능력을 키울 수 있게 된다.



[그림 2] Stop, Slow & Go 프로그램에 참여하는 학생[4)]

4) https://www.funacademy.fi/post/digital-safety-and-the-success-of-online-workshops-stop-slow-go

다. 사이버 범죄 출구(Cybercrime Exit) 프로그램

디지털 범죄 가해 학생을 위한 프로그램 또한 진행되고 있다. 핀란드 경찰청이 주관하는 '**사이버범죄 출구' 프로그램은 해킹 등 정보 시스템을 대상으로 한 사이버 범죄를 저질렀거나 그러한 위험성이 있는 청소년에게 도움을 제공**한다. 프로그램 참여는 자발적이며 각 청소년의 상황을 고려하여 개별화된 평가와 지원 제공된다. 프로그램을 통해 학생들은 일반적인 디지털 생활과 디지털 범죄행위의 경계를 인식시키고, 디지털 환경에 대한 긍정적인 시각과 올바른 활용 방법을 익혀 책임감 있는 디지털 전문가로 성장할 수 있는 기회를 얻게 된다. 이 과정에서 학교, 지역 경찰, 사회복지사, 청소년 전문가, 정보보안 기업 등이 협력하여 디지털 범죄 가해 청소년의 범죄 예방과 재사회화를 지원하고 있다.

4. 디지털 범죄 예방을 위한 교사 연수와 지원

주지하다시피 핀란드가 교육 선진국으로 자리 잡을 수 있었던 것은 교사의 역할이 컸다. 핀란드에서 교사는 하나의 교육 전문가로서 존중받는다. 이와 같은 사회적 상황 속에서 핀란드 교육 당국은 교사들의 역량을 키우기 위해 많은 노력을 기울이고 있으며, 디지털 범죄 예방 영역에서도 다르지 않다. 핀란드에서는 교사가 디지털 시대의 위험과 교육 방법을 충분히 파악할 수 있도록 지원하고 있다. **교원 양성 과정에서부터 미디어 교육과 디지털 윤리가 다루어지고 있음은 물론이고 현직 교원을 위한 다양한 연수 역시 제공된다.** 또한 핀란드 교육부는 현장 교사들을 위한 온라인 자료 플랫폼을 운영하여 수업에 활용할 수 있는 미디어 리터러시 수업자료와 가이드를 공유하고 있어 현장 교사들은 사이버 괴롭힘 대응 수업자료, 딥페이크 관련 교육자료, 개인 사진 공유 및 개인정보보호 교육자료 등 현안별 교육콘텐츠를 쉽게 구할 수 있다.

교원 연수는 대학과 연수원 그리고 관련 단체 등이 협력하여 이루어진다. 특히나 **'핀란드 아동복지연맹', '세이브더칠드런 핀란드' 등 아동 관련 단체가 적극적으로 교사 연수에 참여하고 있다.** 이들은 학교로 찾아가는 교사 연수를 지원하며, 최신 사이버 범죄 동향과 예방 지침을 교육 현장과 공유한다. 핀란드 아동복지연맹은 교사들이 학생의 실제적 삶에서 이뤄지는 디지털 생활 양식을 이해하고 학생들의 입장에서 지도할 수 있도록 돕는 디지털 범죄 대처 연수와 학부모와 함께하는 연수를 제공하고 있다. 세이브더칠드런은 아동 성착취 예방을 위한 교직원 연수 프로그램을 통해 교사들이 성적 이미지 유포나 디지털 그루밍 범죄[5] 징후를 파악하고 적절하게 대응할 수 있도록 돕고 있다. 이와 같은 관련 단체를 통한 연수 프로그램들은 정부의 보조금 지원을 받아 이루어진다. 교육부는 매년 미디어교육 및 리터러시 증진을 위한 프로젝트에 예산을 지원하여 교원의 디지털 범죄 예방 교육 역량 강화를 지원한다.

5) 가해자가 피해자를 길들여 성폭력을 용이하게 하거나 은폐하는 행위, 범죄를 수월하게 하고 범죄의 폭로를 막으려고 대인관계 및 사회적 환경이 취약한 대상에게 다양한 통제 및 조종 기술을 사용하는 범죄행위.

5. 디지털 범죄 예방을 위한 지역사회의 노력

핀란드에서는 디지털 범죄 예방을 위한 지역사회와의 협력 또한 활발하게 이뤄지고 있다. 2024년 9월에는 여러 관련기관이 공동 주최한 **'알아차리고, 배우고, 신고하자(Recognize, Learn, Report!)' 캠페인이 진행되었다.** 이 캠페인은 종합학교 7~9학년을 대상으로 일주일간 소셜미디어를 통해 진행되었다. 캠페인 이름에서 알 수 있듯이 학생들이 디지털 환경에서 일어나는 범죄를 스스로 인식하고 대처하는 방법과 문제가 발생했을 때 이를 신고하는 절차를 교육하였다. 캠페인 기간 동안 지역사회와 참여 기관은 청소년들에게 익숙한 콘텐츠를 활용하여 디지털 그루밍, 사이버 괴롭힘 등 여러 디지털 범죄를 설명하고 퀴즈 이벤트를 열어 참여를 독려하였다.

핀란드 경찰은 디지털 범죄 예방을 위해 디지털 소통 창구를 넓히기 위해 노력하고 있다. 2025년 2월 **핀란드 경찰은 인스타그램, 틱톡, 스냅챗 등 학생들이 많이 사용하는 소셜미디어에서 디지털 범죄 예방 주간 캠페인을 진행하였다.** 캠페인 동안 경찰관들이 직접 라이브 채팅을 열어 청소년들의 질문에 답하고 유익한 정보를 제공하였는데, 관련 게시물들이 수백만 회의 조회수를 기록하는 등 큰 호응을 얻었다. 또한 일부 청소년들은 경찰에게 개인적인 피해 사례를 익명으로 상담하기도 하여 학생들의 디지털 범죄 예방과 해결을 위한 실제적 효과를 거두었다. 이와 같은 과정을 통해 핀란드의 경찰은 청소년들에게 디지털 범죄 예방과 해결을 위한 신뢰받는 파트너로 다가가 범죄 예방은 물론 범죄 피해 신고를 독려하는 역할을 수행할 수 있었다. "청소년들이 온라인에서 많은 시간을 보내는 만큼, 우리도 그 공간에서 함께하며 안전망이 되어주고자 한다."는 경찰 관계자의 발언은 핀란드 디지털 범죄 예방을 위한 그들의 방향성을 보여준다.

지역사회의 중요한 구성원인 민간단체 또한 디지털 범죄 예방을 위해 노력하고 있다. 핀란드의 아동 단체인 **'Protect Children'은 청소년들이 디지털 범죄에 노출된 또래 피해자를 돕는 방법을 알려주는 #MyFriendToo 캠페인을 운영**하여 친구가 디지털 성범죄 피해를 당했을 때 안전한 어른에게 알리도록 권장하고 필요한 정보를 공유하고 있다. 이는 핀란드에서 디지털 범죄 피해 학생들이 피해 사실을 주로 친구에게만 털어놓고 정작 어른이나 교육 기관에는 알리지 않는 경향을 보인 것에서 기인하였다. 또래 집단과 함께 도움을 제공할 수 있는 어른 및 기관의 자신의 피해 사실을 알리는 문화를 만듦으로써 학생들의 피해 사실이 묻히지 않고 도움을 줄 수 있는 공간으로 드러날 수 있도록 한 것이다.

[그림 3] #MyFriendToo 캠페인 포스터[6)]

6) https://www.suojellaanlapsia.fi/en/myfriendtoo

6. 맺음말

핀란드의 디지털 범죄 예방 교육은 단지 정보 제공이나 기술적 대응을 넘어 학생들이 디지털 공간에서 자신을 보호하고 타인을 존중하며 책임감 있는 시민으로 살아갈 수 있도록 돕는 통합적 접근 방식을 보여준다. 유아기부터 고등학교에 이르기까지 전 생애 단계에 걸쳐 이루어지는 미디어 리터러시 교육, 교과와 비교과를 아우르는 디지털 안전 교육, 그리고 교사 연수와 지역사회 협력 등 핀란드는 **디지털 시대의 변화에 맞춰 디지털 범죄 예방을 위한 교육적 생태계를 구축**해 가고 있다.

특히 핀란드는 사이버 괴롭힘, 디지털 성범죄, 딥페이크 등 점점 정교해지는 디지털 범죄 양상에 대응하기 위해 예방, 발견, 대처, 회복 등 **디지털 범죄 예방 및 해결 과정 전체를 포괄하는 안전망을 마련해 학생들을 보호하고 있다.** 여기에는 학생뿐 아니라 학교, 교사, 학부모, 지역사회, 경찰, 민간단체 등 모든 주체가 함께 책임을 나누고 협력하는 사회적 문화가 바탕이 되고 있다.

핀란드의 사례는 우리 교육 현장에도 중요한 시사점을 제시한다. 점차 복잡해지는 디지털 환경에서 디지털 범죄 예방과 학생 보호는 기술의 문제가 아니라 교육의 문제이며 단속이 아닌 공감과 참여 그리고 신뢰를 바탕으로 한 예방 교육이 핵심이 되어야 한다. 우리 교육 역시 학생들이 디지털 공간에서 자신을 지키고 주체적으로 살아갈 수 있도록 교육의 역할과 방향을 고민하고 있다. 이러한 상황에서 핀란드의 경험과 그 방향성은 우리에게 많은 생각거리를 제공한다.

【참고 자료】

- EU Youth WIKI, Media literacy and safe use of new media
  https://national-policies.eacea.ec.europa.eu/youthwiki/chapters/finland/68-media-literacy-and-safe-use-of-new-media
- Welivesecurity, Finland – hope in the fight against cyberbullying
  https://www.welivesecurity.com/2016/07/26/cyberbullying-finland-kiva/
- Finish Government, The “Recognise, learn, report!” campaign seeks to prevent crime taking place online
  https://valtioneuvosto.fi/en/-/25235045/the-recognise-learn-report-campaign-seeks-to-prevent-crime-taking-place-online
- UNESCO, education-profile Finand
  https://education-profiles.org/europe-and-northern-america/finland/~technology

영국의 딥페이크 등 디지털 범죄 예방 교육

발간위원 : 정기엽 (청송중학교부동분교장 교사)

AI 기술의 급속한 발전과 함께, 영국 내 청소년들이 직면하는 디지털 위협의 양상도 점차 다양해지고 있다. 이에 따라 영국 교육계는 사이버 범죄에 대한 인식을 제고하고, 학생들이 안전하고 책임 있게 디지털 환경을 활용할 수 있도록 다층적인 대응 체계를 마련하고 있다.

1. 영국 내 청소년 사이버 범죄의 증가

영국 국가범죄수사국(NCA)의 보고서 『Youth Pathways into Cyber Crime in the UK』(2022)에 따르면, 청소년들이 디지털 범죄에 처음 노출되는 평균 연령이 2017년 대비 낮아진 것으로 나타났다. 특히 청소년은 다음과 같은 다양한 형태의 사이버 범죄에 취약한 것으로 분석된다.

- ◆ 온라인 괴롭힘(사이버 불링): 소셜 미디어 플랫폼을 통한 지속적인 괴롭힘
- ◆ 신원 도용 및 금융 사기: 타인의 개인정보를 무단으로 수집해 금전적 이득을 취하는 행위
- ◆ 해킹 및 무단 접속: 타인의 계정이나 시스템에 대한 불법 접근 시도
- ◆ 악성코드 배포: 바이러스나 스파이웨어 등을 직접 제작하거나 유포
- ◆ 온라인 유인(Grooming): 온라인상에서 청소년이 성적 유인의 피해자 또는 가해자가 되는 경우
- ◆ 부적절한 이미지 공유: 또래 간 음란 이미지 또는 영상을 비자발적으로 공유하거나 유포

더 우려스러운 점은, 이러한 사이버 범죄가 청소년에게 '이중적 성격'을 부여한다는 점이다. 즉, 청소년은 피해자이면서 동시에 가해자가 되기도 한다. NCA의 Cyber Choices 프로그램에 따르면, 십대들이 해킹, DDoS(서비스 거부 공격), 심지어 악성코드 개발 및 배포에까지 관여한 사례가 다수 보고되었다. 많은 경우, 이들은 자신들의 행위가 법적으로 어떤 결과를 초래하는지, 그리고 피해자에게 어떤 영향을 미치는지 제대로 인식하지 못하고 있다는 점에서 교육적 개입(介入)이 더욱 절실하다.

2. 딥페이크: 새로운 위협의 부상

딥페이크(Deepfake)는 인공지능 기술을 활용해 실제 인물의 얼굴, 목소리, 말투 등을 정교하게 모방한 가짜 콘텐츠를 만들어내는 기술이다. 초기에는 오락 목적의 영상 합성에 국한되었지만, 최근에는 음성 모사, 실시간 영상 변조, 텍스트 기반 AI 합성 등 다양한 형태로 확장되며, 그 악용 가능성 역시 빠르게 증가하고 있다. 영국 국가사이버보안센터(NCSC)의 2024년 연례 보고서에서는 딥페이크를 포함한 인공지능 기반 사이버 위협의 증가, 청소년을 대상으로 한 사이버 범죄의 심각성을 강조하고 있다.

딥페이크 기술은 다음과 같은 방식으로 악용되고 있다.

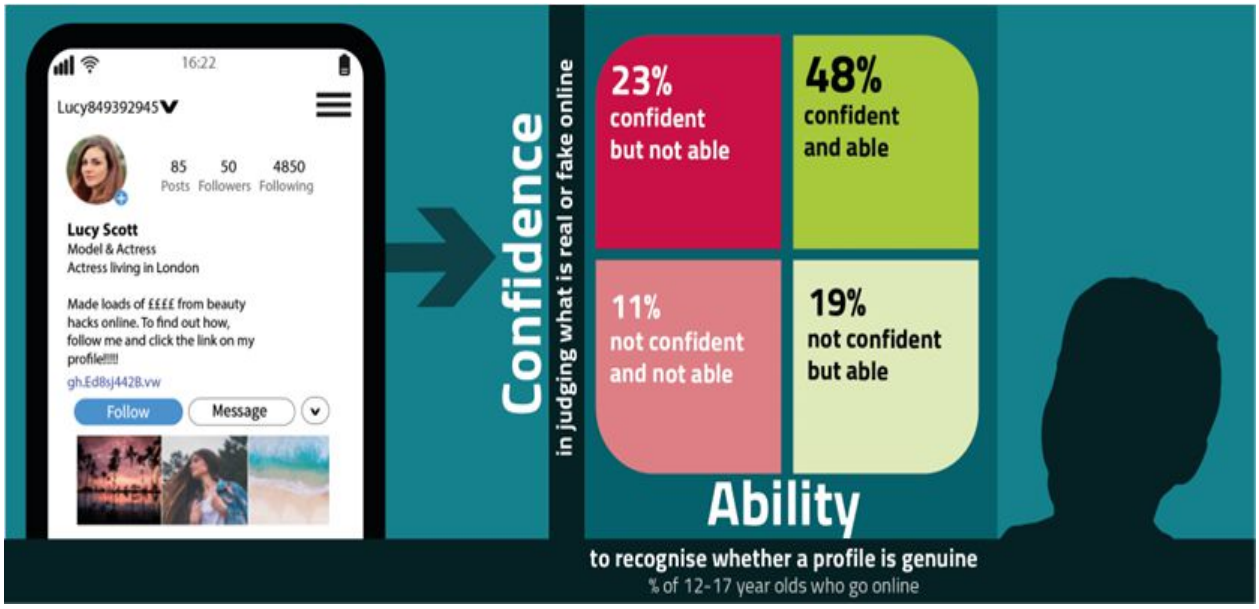
◆ 이미지 기반 괴롭힘: 친구나 교사의 얼굴을 영상에 **합성**해 유포, 심각한 정신적 피해 유발

◆ 신원 사칭: 청소년의 얼굴과 **목소리를 모방**하여 금전 요구, 가족 대상 보이스피싱 시도

◆ 온라인 명예 훼손: 특정 학생의 평판을 훼손하는 **조작 영상** 유포, 가짜 뉴스 제작

◆ 사회적 왜곡 콘텐츠 제작: 기술에 대한 호기심으로 딥페이크 콘텐츠를 **실험, 생성, 유포**

이러한 행위들은 단순한 기술 오용을 넘어, 개인 권리 침해와 명예 훼손, 법적 책임이 수반되는 중대한 윤리적·법적 문제로 확산되고 있다.



[그림1] Children and Parents: Media Use and Attitudes(2023)

3. 교육 현장의 대응 전략

가. 교육과정 통합

영국의 국가 교육과정은 2014년 개정 이후부터 디지털 리터러시를 포함하고 있으며, 2019년과 2023년에 추가로 개정되었다. 2014년부터 컴퓨팅 교육은 초등학교부터 필수로 편성되었으며, 온라인 안전과 책임 있는 디지털 시민의식을 다루는 모듈도 포함되어 있다. 학생들은 단지 기술을 사용하는 법뿐만 아니라, 윤리적이고 안전한 사용법도 배우고 있다.

CyberSprinters 프로그램

주관: National Cyber Security Centre (NCSC, 영국 국가사이버보안센터)

대상: Key Stage 2 (초등학교 고학년)

내용: 사이버 범죄의 기본 개념 소개 (예: 피싱, 비밀번호 보호, 소셜 엔지니어링)
인터랙티브 게임, 퀴즈, 캐릭터 기반 이야기를 통해 보안 습관 함양
교사용 가이드와 활동지 포함

특징: 놀이 기반 접근으로 디지털 안전 교육의 진입장벽을 낮춤

자료: CyberSprinters Practitioner Guide (NCSC)

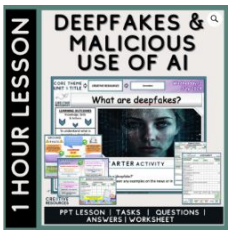
PSHE(Personal, Social, Health and Economic education) 수업

주관: PSHE Association + 외부 리소스 제공 업체 (TES, Cre8tive Resources 등)

대상: Key Stage 3~4 (중등학교)

내용: 딥페이크 영상 시청 → 진위 여부 판단 퀴즈
AI가 생성한 이미지와 실제 이미지 구별하기
딥페이크의 피해 사례(유명인 합성, 학교폭력, 협박 등) 분석
피해 신고 및 대응법 토론

자료: Deepfakes, AI and Online Safety (TES)
Rise of Deepfakes and Malicious AI (Cre8tiveResources)



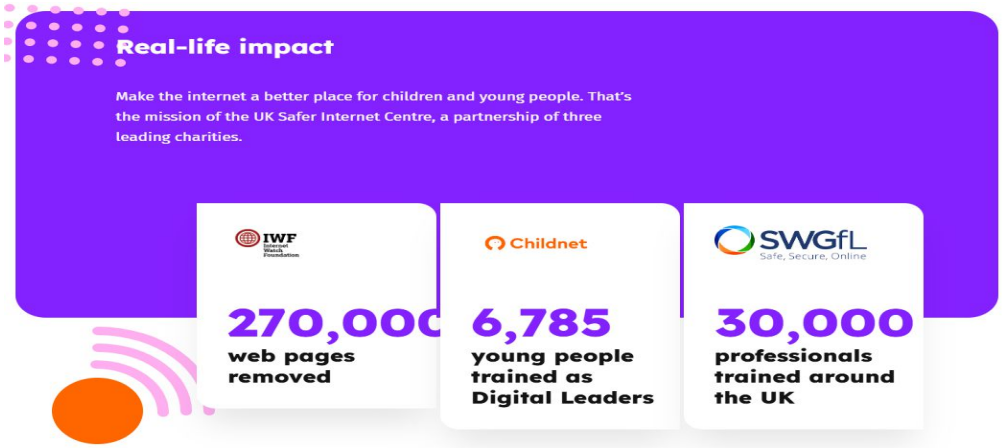
나. 정책적, 기술적 대응 및 교직원 연수

보호 정책 수립	기술적 솔루션	교직원 연수 및 인식 제고
• 온라인 사건 보고를 위한 명확한 절차 • 기술 사용에 대한 지침 • 사이버 불링 사례 관리 절차 • 온라인 학대 피해자 지원 전략	• 부적절한 웹사이트를 차단하는 콘텐츠 필터링 시스템 • 사이버 보안 위협을 탐지하는 모니터링 소프트웨어 • 인증 절차가 있는 안전한 네트워크 • 정기적인 보안 점검 및 취약점 평가	• 사이버 범죄 피해의 징후 인식 • 신종 온라인 위협 이해 • 온라인 피해를 경험한 학생 지원 • 위험한 온라인 행동에 가담하는 학생 식별

다. 외부 기관 협력

외부기관	주요 활동	학교와의 협력 방식
National Crime Agency (NCA) *Cyber Choices 프로그램 제공*[7]	- 청소년 대상 해킹·딥페이크 등 사이버 범죄 예방 교육 - 법적 결과 인식 및 기술의 긍정적 사용 장려	- 학교 초청 강연 - 컴퓨팅 수업 연계 워크숍 운영 - 실무자와의 Q&A 세션
National Cyber Security Centre (NCSC)	- 온라인 위협에 대한 인식 제고 - 교사 및 학생 대상 사이버 보안 학습 자료 제공 - 딥페이크 대응 매뉴얼 제공	- 연례 보고서 및 교육용 리소스 배포 - 학교 네트워크 보안 점검 가이드라인 제공
Internet Matters	- AI와 SNS 상의 위험에 대한 학부모용 가이드 - 이미지 기반 괴롭힘, 딥페이크 대응법 안내	- 학교와 공동으로 학부모 대상 설명회 개최 - 안전한 디지털 환경 구축을 위한 체크리스트 제공
UK Safer Internet Centre (UKSIC) SWGfL + Childnet + IWF 협력 운영	- 온라인 안전 교육의 중심 기관 - Safer Internet Day 운영 - 수업자료/캠페인/정책 가이드 제공 - 합성 콘텐츠 대응 교육 강화	- 교사용 수업안, 활동지, 퀴즈 제공 - 학년별 맞춤 콘텐츠 배포 - 전국 캠페인 참여 연계 - 신고 시스템(Report Harmful Content) 안내
IWF (Internet Watch Foundation)	- 아동 성착취·딥페이크 음란 이미지 탐지 및 제거 - Report Remove: 피해 이미지 삭제 시스템 운영 - 불법 콘텐츠 해시 DB 전 세계 공유	- 학생 대상 이미지 유출 대응 교육 - 학교 웹사이트·SNS 이미지 관리 가이드 제공 - Report Remove 시스템 안내 포스터/가정통신문 배포 - 교직원 대상 콘텐츠 대응법 안내
Childnet International	- 딥페이크와 관련된 '디지털 발자국' 주제 수업자료 제공 - 초·중·고 맞춤형 온라인 안전 교육	- 학생 대상 참여형 워크숍 - 학부모·교직원 대상 세미나 - Safer Internet Day 공동 캠페인
South West Grid for Learning (SWGfL)	- 딥페이크 및 합성 미디어에 대한 교사 지원 자료 제공 - 온라인 괴롭힘 대응 절차 안내	- 'ProjectEVOLVE'를 통한 커리큘럼 콘텐츠 제공 - 학교 정책 점검 도구 공유
TechSafe Schools Consortium (런던 중심 컨소시엄)	- 딥페이크 식별 기술을 활용한 디지털 포렌식 체험 수업 - AI 기반 사례 분석 훈련	- 현장 전문가와의 실습 기반 워크숍 - 중등학교 중심 실험 프로그램 운영

7) 컴퓨터 혹은 디지털 기술을 적법하게 활용할 수 있도록 돕는 국가 프로그램, https://www.nationalcrimeagency.gov.uk/cyber-choices



[그림2] UK Safer Internet Centre (UKSIC)

라. 관련 법규

딥페이크의 교육 현장 유입을 방지하기 위한 법적 움직임도 병행되고 있다. 2023년 개정된 온라인 안전법(Online Safety Act)은 플랫폼 운영자에게 조작된 영상의 유포를 막을 책임을 명확히 하며, 학교에서 이러한 위험에 대한 교육을 제공하도록 독려하는 가이드라인도 함께 마련되었다.

법률명	주요 내용	딥페이크 및 디지털 범죄 적용 사례	교육 현장 활용
Malicious Communications Act (1988)	협박, 모욕, 괴롭힘 등 유해한 메시지 발송 금지	딥페이크 이미지·영상으로 특정인을 조롱하거나 괴롭히는 경우	사이버 불링 예방 수업에서 괴롭힘 유형과 법적 처벌 소개
Computer Misuse Act (1990)	무단 접근, 해킹, 시스템 손상 행위 금지	조작된 딥페이크 콘텐츠 생성을 위한 해킹, 계정 탈취 시 적용	ICT 윤리 수업에서 '불법 접근'과 '법적 책임' 주제로 활용
Protection from Harassment Act (1997)	지속적인 괴롭힘, 불안 유발 행위 금지	딥페이크 콘텐츠를 반복적으로 퍼뜨리며 피해자를 괴롭힐 경우 적용	반복적 괴롭힘의 법적 기준, 신고 절차에 대한 교육 활용
Data Protection Act (2018) **(UK GDPR 기반)**	개인정보(이미지 포함) 수집·유포 금지	동의 없이 타인의 얼굴·음성을 사용해 딥페이크 제작 시 적용	학생의 초상권 및 이미지 사용 동의 절차 교육 시 반영
Online Safety Act (2023)	온라인 유해 콘텐츠 차단, 플랫폼 운영 책임 강화	딥페이크 음란물·조작 영상 유포에 대해 플랫폼과 가해자 모두 법적 책임	예방 교육 시 플랫폼 책임, 학생 권리, 신고 절차 교육에 활용

4. 맺음말

사이버 범죄 예방 노력은 디지털 전환이라는 더 넓은 사회적 흐름 속에서 중요한 역할을 하고 있다. 최근 몇 년간 국가와 학교 차원에서 추진된 다각적인 접근은 이 위협적인 문제에 점차 적응해 가고 있음을 보여준다. 교육적 이니셔티브, 기술적 보호 조치, 정책 개발, 외부 협력이 결합된 이 전략은 보다 안전한 디지털 환경 조성에 초점을 맞추고 있다.

영국의 교육기관들은 이제 다양한 외부 기관 및 기술기업과의 협력은 물론, 학부모와 학생을 대상으로 한 실질적이고 참여 중심의 교육을 통해 디지털 시민의식을 높이는 방향으로 나아가고 있다. 효과적인 사이버 범죄 예방은 단지 기술적 해결책만으로는 불가능하며, 문화적 인식 변화와 디지털 시민의식 함양이 병행되어야 할 시점이다. 기술 변화의 속도를 쫓기보다는, 교육은 그 변화의 나침반이 되어야 한다.

【참고 자료】

- National Crime Agency (2022). Youth Pathways into Cyber Crime in the UK. https://www.nationalcrimeagency.gov.uk/news/youth-pathways-into-cyber-crime
- National Crime Agency (2023). Cyber Choices Programme Overview. https://www.nationalcrimeagency.gov.uk/cyber-choices
- National Cyber Security Centre (2024). Annual Review 2024. https://www.ncsc.gov.uk/annual-review/2024
- Department for Education (UK). Online Safety Act 2023 Summary. https://www.gov.uk/guidance/online-safety
- Internet Watch Foundation (2023). How AI is being abused to create child sexual abuse imagery. https://www.iwf.org.uk/media/q4zll2ya/iwf-ai-csam-report_public-oct23v1.pdf
- Internet Watch Foundation (2024). What has changed in the AI CSAM landscape? https://www.iwf.org.uk/media/q4zll2ya/iwf-ai-csam-report_public-oct23v1.pdf
- Department for Education (2025). Generative Artificial Intelligence (AI) in Education https://www.gov.uk/government/publications/generative-artificial-intelligence-in-education/generative-artificial-intelligence-ai-in-education

프랑스의 딥페이크 등 디지털 범죄 예방 교육

발간위원 : 이한길 (포항제철지곡초등학교 교사)

프랑스 청소년들의 삶에 디지털 기술이 깊숙이 자리 잡으면서 새로운 사회적 문제들이 발생하고 있다. 디지털 범죄는 기술적 문제를 넘어, 기존의 폭력과 차별 등 사회적 역학 관계를 디지털 공간에서 반영하고 증폭하는 현상으로 나타나고 있다. 특히, 학생들 사이 디지털 폭력 사례가 증가하면서 프랑스에서도 이를 교육적 맥락에서 집중적으로 분석, 대응하고 있다. 이는 디지털 범죄가 해킹이나 사기 같은 수준을 넘어, 교육 환경에 직접 피해를 미치는 대인 공격 형태로 진화했기 때문이다. 이에 프랑스가 추진하고 있는 다양한 대응 정책과 체제를 살펴보고자 한다.

1. 디지털 폭력 현황 및 법적 대응

가. 다양한 디지털 폭력 유형

디지털 폭력의 유형은 첫째, 디지털 폭력과 괴롭힘(Cyberharcèlement moral)으로, 온라인상에서 반복적으로 이루어지는 협박, 모욕, 조롱, 위협, 따돌림 등을 포함한다. 이는 단순한 일회성 사건과 구별되며, 반복성과 가해자와 피해자 간의 힘의 불균형을 주요 특징으로 한다. 둘째, 디지털 성차별과 성희롱(Cyberharcèlement sexuel)으로, 원하지 않는 성적이거나 성차별적인 콘텐츠를 전송하거나, 리벤지 포르노(pornodivulgation), 성적 문자 메시지 전송(sexting), 성적 모욕(slut-shaming, body-shaming), 성별이나 성적 지향에 따른 표적화 행위 등을 포함한다. 이는 특히 여학생이 피해자인 경우가 많다. 이외에도 또래 간 문제를 넘어 신원 도용 및 사칭(Usurpation d'identité), 폭행 장면 촬영 및 유포, 불필요한 온라인 논쟁 유발, 개인 정보 유포, 웹캠 협박 등도 존재한다.

나. 디지털 폭력 규모, 대상 현황 통계

최근 프랑스 교육부 평가예측성과국(DEPP)의 2023년 조사에 따르면, 학교 괴롭힘의 영향을 받

은 학생 비율은 초등학교(CE2-CM2) 5%, 중학교(collège) 6%, 고등학교(lycée) 4%에 달한다. 조사 내용을 더 구체적으로 살펴보면, 중학생 5명 중 1명이 디지털 폭력을 경험했고, 중학생의 4.5%는 반복적인 괴롭힘에 시달린 것으로 나타났다. 또한 e-Enfance 협회에 따르면, 전체 가정의 20~24%가 디지털 괴롭힘 상황을 경험한 적이 있다고 한다. 특히 2024년 조사에서는 아동의 23%가 디지털 폭력을 경험한 것으로 보고되어, 2023년의 18%보다 피해 규모가 뚜렷하게 증가했음을 알 수 있다. 프랑스 학생들이 OECD 평균보다는 디지털 폭력에 덜 노출되었다고 평가할 수도 있지만, 연간 약 50만 명에 이르는 피해 규모가 적지 않다. 이 가운데 특히 눈에 띄는 것은 '취약 집단'에 대한 조사 결과이다. LGBTQ+ 학생, 장애 학생, 피부색이 다수 학생과 다른 학생은 피해율이 높고 지원받을 가능성도 상대적으로 낮다는 점이 심각한 문제로 부각되고 있다.

다. 법적 대응

프랑스의 법체계는 청소년 대상 디지털 범죄 위협에 대응하여 꾸준히 진화하고 있다. 구체적인 법률과 가중 처벌 조항들이 마련되어 있지만, 디지털 플랫폼과 온라인 행태가 빠르게 변화하기 때문에 법이 충분한 실효성을 발휘하기 어렵다는 지적이 있다. 즉, 법은 피해를 구체적으로 규정하려 하지만, 디지털 환경이 지속적으로 변하고 있기 때문에 이에 따른 법적, 정책적 대응 역시 지속적인 개선이 요구되는 상황이다.

디지털 괴롭힘은 프랑스 형법상 정신적 괴롭힘의 가중 처벌 사유(형법 제222-33-2조)로 명시되어 있으며, 학교 괴롭힘 또한 2022년 3월 2일 제정된 법률에 따라 특정 범죄로 인정받고 있다. 정신적·성적 디지털 괴롭힘에 대해서는 상세한 처벌 규정이 마련되어 있으며, 피해자 및 가해자의 연령에 따라 처벌의 경중이 달라진다. 특히 피해자가 15세 미만 미성년자이거나 괴롭힘으로 인해 피해자가 자살에 이른 경우에는 최대 10년의 징역형까지 받을 수 있다. 이외에도 초상권 침해나 신원 도용 등 별도의 처벌 규정도 존재하며, 온라인 플랫폼 운영자에게는 유해 콘텐츠의 신속한 삭제 책임과 가해자 계정 차단의 의무도 부과하고 있다.

디지털 폭력은 종종 학교 내 갈등 상황에서 비롯되지만, 시간이 지남에 따라 온라인으로 확대되어 지속적인 폭력의 형태로 이어진다. 이러한 현상은 법적 개입의 경계를 모호하게 만들고, 온라인이나 오프라인 어느 한쪽만을 대상으로 한 단편적 해결책이 적절하지 않음을 보여준다. 즉, 효과적인 예방과 대응은 단순히 디지털 기술 활용에만 의존할 것이 아니라, 학교 공동체 내에서 발생하는 갈등과 폭력의 근본적 원인을 함께 해결해야 한다는 것을 강조한다.

2. 프랑스 교육부의 대응

프랑스 교육부는 청소년 대상의 디지털 폭력과 괴롭힘 문제에 대응하기 위해 법적·교육적·기술적·사회적 차원의 협력을 통합한 접근 방식을 채택하고 있다. 구체적으로는 법률 제정 및 부처 간

협력 체제 구축, 초·중·고등학교에서의 공통적인 pHARe 프로그램 시행, 3018 전용 상담 전화 운영, 외부 파트너와의 연계 및 협력 강화 등을 중심으로 정책을 전개하고 있다. 세부 내용은 다음과 같다.

가. 입법 대응 및 부처 간 협력

프랑스는 2022년 법률을 통해 학교 괴롭힘 및 디지털 괴롭힘을 특정 범죄로 법적으로 인정하고, 기존의 형법 조항을 적용해 처벌의 실효성을 높였다. 이어 2023년에는 교육부, 법무부, 경찰 및 헌병대, 디지털 정책 관련 부서, 보건부와 체육부 간의 협력을 특히 강조했다. 구체적인 조치로는 심각한 사안을 검찰에 직통으로 보고하는 시스템 구축, 법원 및 지역 위원회에 전담 담당자 배치, 고소 접수를 위한 공동 평가 기준 마련, 학교 내 경찰 개입 활성화, 온라인 플랫폼과의 협력 강화 등을 들 수 있다. 이를 뒷받침하기 위해 삼천만 유로의 예산을 증액하고, 괴롭힘 방지 여단(FTE) 소속 인력 150명과 전담 조정관을 별도로 배치하였다.

나. pHARe(un programme de lutte contre le harcèlement à l'école) **프로그램 시행**

pHARe 프로그램은 2023학년도부터 프랑스 모든 초·중·고교에서 의무적으로 시행된다. 교육 및 예방, 보호 공동체 형성, 효과적 개입, 학부모·파트너 참여, 학교 민주주의 기구 활용 등 다섯 가지 핵심 원칙을 기반으로 운영된다. 각 학교는 지역 내 다양한 전문 인력과 협력하여 사안 처리팀을 구성하고, 학생 대사(élèves ambassadeurs)를 지원하며 파트너 대상 교육을 실시한다. 프로그램은 CP부터 Terminale까지 연간 열 시간 학습이 필수이며, 예방 교육과 더불어 사회정서 역량(공감, 의사소통, 감정 조절, 문제 해결, 비판적 사고 등) 개발 및 디지털 폭력에 대한 이해를 강조한다. 단순 정보 제공이나 처벌적 접근에서 벗어나 괴롭힘의 사회정서적 원인을 다루는 교육적 전환을 지향하며, 학생의 정서 지능 향상과 긍정적 사회적 기술 함양을 통해 학교 문화를 변화시키고자 한다. 중·고교에서는 훈련받은 자원봉사 학생들인 '학생 대사'가 또래 상담을 맡아 상황 보고 및 긍정적 분위기 조성 역할을 수행한다. 학부모에게도 디지털 폭력 인식 개선 워크숍과 정보 제공, 사례 처리 프로토콜(피해자 보호, 조사, 제재, 후속 조치 포함)에 참여하기를 요청한다. 일부 지역에서는 공유 관심사 방법(MPPFR) 같은 특정 방법론을 적용한다. 교원을 위해 디지털 플랫폼인 pHARe는 사안별 대응 방법뿐 아니라 법·제도적 지원과도 연계되어 있다. 또, 디지털 폭력 예방과 해결 노력을 공식적으로 인증하는 세 단계 인증 체제(참여, 심화, 전문)도 운영한다.

[그림1] pHARe프로그램 안내문

[그림2] 3018 디지털 폭력 피해 전용 상담 전화

[그림3] 디지털 폭력에 저항하는 학생 대사(大使)

〈표 1〉 pHARe 프로그램의 주요 구성 요소 및 활동 (참고 문헌을 토대로 집필자가 작성)

축/원칙	활동	대상	실행 수준
교육/예방	연간 10시간 학습 (사회 정서적 역량, 괴롭힘 예방)	학생 (CP ~ Terminale)	모든 학교/기관
	학생 대사 양성 및 활동	중/고등학생	중/고등학교
	주요 행사 참여 (괴롭힘 반대의 날 등)	학생, 교직원	모든 학교/기관
보호 공동체 형성	다양한 직종의 자원팀 구성 및 교육	교직원(최소 5명/지역/기관)	모든 지역/기관
	전 교직원 대상 교육 (2027년까지 100% 목표)	모든 교직원	모든 학교/기관
효과적인 개입	표준화된 개입 프로토콜 적용 (피해자 보호, 조사, 제재, 후속 조치 포함)	교직원, 자원팀	모든 학교/기관
	3018/3020 핫라인 연계 및 활용	학생, 학부모, 교직원	국가/지역/학교
학부모/파트너 참여	학부모 대상 인식 개선 워크숍 및 정보 제공	학부모	모든 학교/기관
	외부 파트너(협회, 지자체 등)와의 협력	학교/기관	지역/학교
학교 협의기구 활용	학생회(CVC, CVL), 보건/시민/환경 교육 위원회 동원	학생 대표, 교직원	중/고등학교
학교 풍토 측정	학교 풍토 진단 도구 활용	학교/기관	선택적
영향 추적	프로그램 활동 및 결과 모니터링	학교/기관, 지역	지역/국가
자원 플랫폼	pHARe 디지털 플랫폼 제공	교직원	국가

다. 지원 조치: 전용 상담 전화 운용, 디지털 시민성과 디지털 보안 교육

3018 전용 상담 전화는 디지털 괴롭힘 대응에서 핵심적 기능을 수행한다. 특히, 3018 운영자는 온라인 콘텐츠 삭제를 요청할 수 있는 신뢰할 수 있는 신고자(signaleur de confiance)라는 독자적 지위를 부여받으며, 채팅과 증거 저장 기능을 탑재한 전용 앱도 제공받는다. 이와 더불어 지역 및 부서 간 협력 네트워크의 중심 통로로 자리 잡고 있다. 다만, 청소년 대상층의 낮은 인지도와 이용률로 인해 그 효과가 제한적일 수 있다. 이는 홍보를 확대하고 신뢰를 구축하여 소통 격차와 신뢰 문제를 해소할 필요성을 보여주는 부분이다. 디지털 시민성과 디지털 보안 교육은 교육과정(EMC, SNT, NSI 등)에 체계적으로 통합하여 진행하고, Pix 인증(6학년 필수 인증으로 개인 정보 보호 및 디지털 괴롭힘 예방 강조)과 더불어 ANSSI, Cybermalveillance.gouv.fr, CNIL 등의 전문 자원을

적극 활용한다. 이외에도 디지털 시민성 현장 선포 및 초·중학교 내 휴대전화 사용 금지 조치 또한 중요한 예방 전략으로 시행되고 있다.

라. 외부, 기타 파트너와의 협력

학교와 같은 교육기관의 역량만으로 이러한 대응과 교육이 어려우므로, e-Enfance(3018 전화 운영), CLEMI(미디어 리터러시), MAE(보험 및 예방), Apf France handicap, Les Papillons 같은 기관들이 온, 오프라인에서 다양한 자원을 제공하고, 관련 교육을 하며, 지원 활동에 있어 핵심적 역할을 감당한다. 이러한 기관들은 학교 내 활동을 위한 협회 인증 제도(agrément)에 따라 이질적인 두 기관 간 협력 관계를 맺기도 한다. 또한 사법 기관, 경찰, 보건 기관, 디지털 기관과 협회를 구성하는 절차가 마련되어 있다. 다만, 그 과정이 복잡하여 서로 다른 권한과 문화를 가진 기관들 사이에 원활한 정보의 흐름, 공감대 형성, 합의된 기준에 따른 조치를 보장하는 지속적 거버넌스 구축이 필요하다. 이는 각기 다른 우선순위와 절차, 데이터 시스템을 가진 다양한 주체 간의 조정과 협력을 지속적으로 요구하는 과제로 남아있으며, 교육 기관과 사법 기관 간의 전용 플랫폼 구축과 명확한 역할 분담 체계 확립 등을 위한 꾸준한 노력을 요구되고 있다.

3. 프랑스 교육부의 정책적 대응에 대한 평가, 과제

가. 독립적/영향 평가 부재 비판

언론 보도나 공공기관이 발간한 자료를 종합해 보면, pHARe 프로그램이 관련 문제 발생률을 낮추었는지, 학생들의 상황을 실제로 개선했는지 검증하는 대규모 독립적 영향 평가는 찾아보기 어렵다. 최근 프랑스 교육부 산하 평가예측성과국(DEPP)이 실시한 평가는 학생 개인 수준에 초점을 맞추고 있어, 프로그램의 효과를 직접적으로 평가했다고 보기는 어렵다. 교육구(Cités Éducatives)에 대한 청소년·대중교육연구원(INJEP)의 평가는 일부 연관성이 있지만, 이는 pHARe와 별개인 정책이다. 관련 접근 방식이 높은 문제 해결률을 보이더라도, 실제 피해 발생률이나 피해 감소율을 입증할 수 있는 평가는 부재하다고 하겠다. 곧, 현재의 평가는 내부 운영 지표나 자기 보고식 자료에 의존하는 듯하여 프로그램의 실질적 성공 여부를 판단한다고 보기는 어렵다.

나. 개선을 위한 과제

‘100% 학교 참여, 100% 교직원 교육, 100% 상황 처리’라는 pHARe 정책의 핵심 목표는 이상적이지만, 교사 연수 부족, 자원 미비, 실행의 일관성 결여 등 현실과 상당한 괴리를 보인다. 이러한 불일치는 정책 목표와 시스템의 실제 역량 간 간극을 드러내며, 디지털 범죄에 대한 교육부의 대응이 실효를 거두지 못할 가능성을 시사한다. 구조적 조정과 개선된 실행 방안 개선이 필요한 이유이다. 개선을 위한 첫 번째 과제는 교직원 연수이다. 디지털 괴롭힘의 심각성과 파급력은 커지

고 있지만, 이를 대응할 인원과 자원이 턱없이 부족하다. 해당 영역의 실무에 대한 교사의 자신감 부족, 문제 해결을 위한 시간적 제약 등은 시급히 보완해야 할 과제로 지목되며, 이를 극복하기 위한 전문성 강화 노력이 우선순위로 부각 되고 있다. 이에 프랑스 정부는 2027년까지 전 교직원 대상 연수 완료를 목표로 제시했다. 두 번째 과제는 자원 배분이다. 프로그램의 효과적 실행을 위해서는 충분한 인적, 재정적 자원이 확보되어야 한다. 특히 교육 심리학자, 사회복지사 등 전문 인력과의 협력 방식, 역할 분담을 명확히 하고, 이들을 현장에 적절히 배치하기 위한 구체적 조치가 필요하다. 취약 계층 학생을 제도권에서 온전히 포용하고, 학부모의 실질적 참여를 유도하려는 노력도 함께 요구된다. 피해자 지원 창구인 3018의 인지도 제고를 위한 온, 오프라인 홍보도 지속적으로 해야 한다고 말한다. 끝으로, 개입 과정의 제도적 복잡성 해소가 과제이다. 가해자 식별, 증거 수집, 개인 정보 보호, 집단 역학의 관리 등은 핵심적 단계들이지만, 절차가 복잡하고 일관되지 않다는 문제가 있다. 따라서 협력 체계의 재정비와 절차 간소화가 요구되며, 동시에 효과성을 유지할 수 있는 체제 개선이 정책 성패를 좌우할 핵심 과제로 떠오르고 있다.

4. 맺음말 및 시사점

디지털 환경의 확산은 청소년의 사회적 상호작용에 새로운 가능성을 열어주었지만, 동시에 심각한 위험도 초래하고 있다. 특히 사이버 폭력은 정신 건강, 학업 성취, 사회성 발달에 부정적인 영향을 미치는 큰 문제로 부상했다. 이에 프랑스 교육부는 법적 대응 강화, 부처 간 협력 체계 구축, pHARe 프로그램의 전국적 의무 시행으로 체계적 대응 의지를 분명히 하고 있다. pHARe 프로그램은 예방 교육, 보호 공동체 형성, 효과적인 개입, 학부모 및 외부 파트너의 참여, 학생 주도 활동 등 다각적인 접근을 기반으로 운영되고 있고, 3018 전용 상담 전화 같은 지원 체계, 디지털 시민성 교육 강화 역시 핵심 정책 수단으로 활용되고 있다. 이러한 노력에도 불구하고 여러 과제는 여전히 있는데, 정책 효과에 대한 독립적이고 엄밀한 평가가 아직 부족하며, 교직원 교육과 자원의 부족, 지역 및 학교 간 실행 편차, 빠르게 변화하는 디지털 환경에 대한 현장의 대응력 부족 등이 지속적으로 비판받고 있다. 이를 극복하기 위한 정책적 보완이 과제로 남아 있다.

【참고 자료】

- CP_VO_3018eEnfance_V2_08022023-GV.pdf (출처: https://e-enfance.org/)
- https://www.legifrance.gouv.fr/download/pdf?id=T9GT3JsuVT6ecjh8ubxCzvhz-NU-8kPmzOIM-oycfNs
- https://www.education.gouv.fr/rentree-2023-de-nouvelles-mesures-contre-le-harcelement-l-ecole-377852
- https://eduscol.education.fr/3730/charte-pour-l-education-la-culture-et-la-citoyennete-numeriques
- https://www.education.gouv.fr/strategie-du-numerique-pour-l-education-2023-2027-344263

미국의 딥페이크 등 디지털 범죄 예방 교육

발간위원 : 이호연 (예천여자고등학교 교사)

1. 딥페이크 및 디지털 범죄 예방 교육의 현황과 과제

최근 인공지능(AI) 기술의 발전과 함께 딥페이크를 이용한 디지털 범죄가 빠르게 증가하고 있다. 특히 이미지 합성, 음성 조작, 영상 변조 기술이 정교해지면서 청소년들의 얼굴이나 신체 이미지가 악용되는 사례가 급증하고 있으며, 이는 학습권과 인권을 침해하는 새로운 유형의 범죄로 확산되고 있다. 실제로 미국 전역에서는 고등학생을 대상으로 한 딥페이크 음란물 생성 사건이 발생하고, 그로 인한 정신적 피해와 사회적 낙인이 심각한 문제로 떠오르고 있다. 이러한 대응을 교육 철학의 차원에서 설명한 마리사 파딜라(Marissa Padilla) 미국 교육부 대변인은 "학생들이 단지 피해자가 아니라, AI 시대의 책임 있는 디지털 시민으로 성장하도록 돕는 것이 우리의 목표입니다." (The 19th) 라고 말하며 교육의 목표를 강조했다. 이러한 상황 속에서 미국 교육계는 단순한 기술 대응을 넘어서, 학생 보호와 디지털 시민성 함양을 위한 제도적·교육적 개입을 본격화하고 있다. 연방 교육부는 물론, FBI, 각 주 교육청, 비영리 민간단체들이 협력하여 디지털 리터러시, 정보 보안, 사이버 윤리, AI 콘텐츠 감별 교육을 포함한 포괄적 교육 프로그램을 운영하고 있으며, 이 흐름은 법 제도 개정과 현장 실천을 동시에 이끌어내는 중요한 동력이 되고 있다.

2. 청소년 대상 딥페이크 범죄 사례

가. 펜실베이니아주 Lancaster Country Day School 사건

2024년 11월, 펜실베이니아주의 Lancaster Country Day School에서 두 명의 남학생이 60명의 여학생 얼굴을 AI를 이용해 누드 이미지에 합성한 사건이 발생했다. 이들은 아동 성적 학대 및 아동 포르노 소지 혐의 등으로 기소되었으며, 사건 이후 학부모들은 학교의 대응 부족을 이유로 소송을 제기하였다. 이 사건은 교육 현장에서 딥페이크 범죄의 심각성을 보여주는 대표적인 사례로 평가

된다. 그러나 단순히 사법적 조치나 행정적 책임으로 마무리되기에는 부족하다는 문제의식도 제기된다. 사건 이후 학교는 재발 방지를 위한 절차 검토를 약속했지만, 학생들과 학부모들은 여전히 디지털 범죄에 대한 교육적 대응이 부실하다고 느끼고 있다. 이러한 맥락에서, 학교 현장에서 딥페이크의 위험성과 예방 전략을 다루는 디지털 시민 교육의 필요성이 더욱 부각되고 있다.

나. 뉴저지주 프란체스카 마니(Francesca Mani) 사건

뉴저지주의 Westfield High School 학생 프란체스카 마니는 AI를 이용해 생성된 가짜 누드 이미지의 피해자가 되었다. 그녀는 사건을 접한 직후 "슬퍼할 것이 아니라 화를 내야 한다고 생각했다. 이건 불공평하고, 그냥 넘어갈 수 없는 일이다"라고 말하며, 어머니와 함께 딥페이크 규제 활동에 본격적으로 나섰다. 어머니 도로타 마니는 학교 측의 초기 대응이 미흡했다며, "스냅챗은 몇 초 후에 사라지니 걱정하지 말라는 말을 들었다. 하지만 우리는 모두 스크린샷이나 사진 촬영으로 이미지가 저장될 수 있다는 것을 알고 있다"고 지적했다. 프란체스카와 그녀의 가족은 이 사건을 단순히 개인 피해로 끝내지 않고, 전국적인 대응으로 확대하였다. 워싱턴 D.C.를 방문한 이들은 연방 의회에 딥페이크 이미지에 대한 법적 대응을 촉구하였으며, 그 결과 뉴저지주는 2025년 4월, '비동의 딥페이크 이미지 방지법(Preventing Deepfakes of Intimate Images Act)'을 제정하였다. 이 법은 AI를 이용해 생성된 비동의 성적 이미지의 제작 및 유포를 범죄로 규정하고 있다. 프란체스카는 이후 딥페이크 피해자들을 위한 웹사이트를 개설하고 전국적인 캠페인을 통해 학교 정책과 법률의 개선을 촉구하고 있으며, "이 법은 아무 일도 일어나지 않았다고 무시당한 모든 여성과 10대들을 위한 것이다. 우리는 함께 변화를 만들 수 있다"고 강조하였다. 프란체스카 마니는 딥페이크 기술 규제를 요구하는 청소년 인권 운동의 상징적 인물이 되었다.

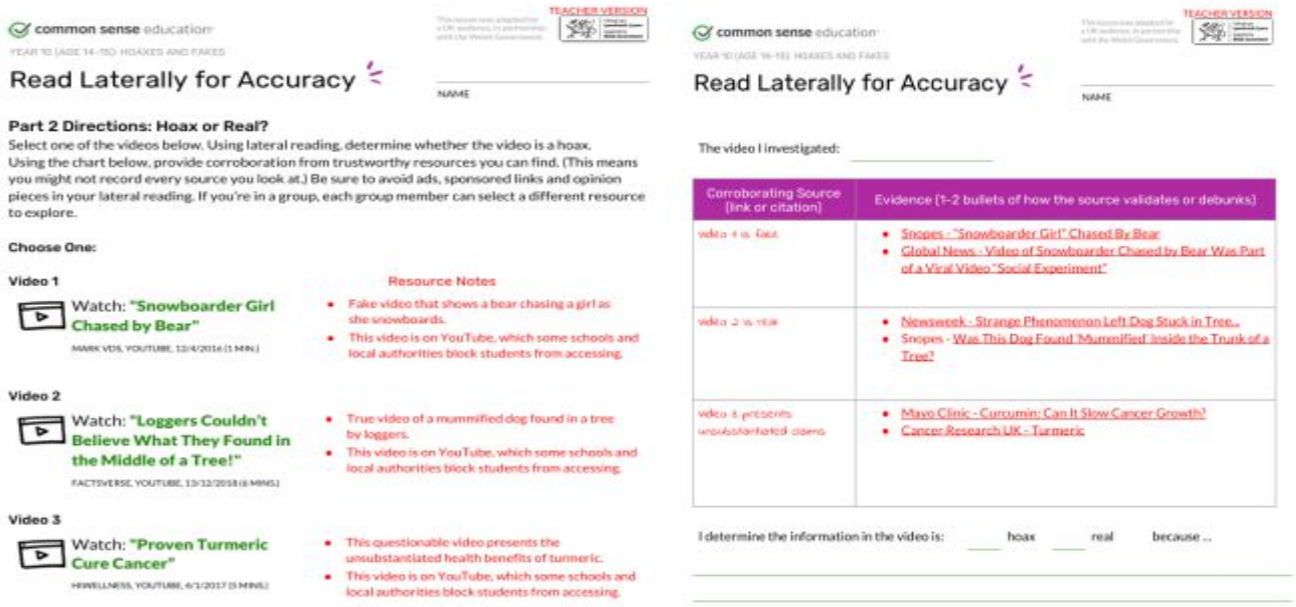
3. 제도적 대응: Title IX 규정 개정과 법적 논의

학생들이 딥페이크 범죄의 직접적인 피해자가 되자, 미국 교육부는 2024년 4월 Title IX 규정을 개정하여 디지털 성희롱의 범위를 확대하였다. 이 개정안은 비동의 딥페이크 이미지의 제작 및 유포를 성희롱의 범주에 포함시켜, 학교가 이를 방치할 경우 책임을 지도록 명시하였다. 미국 교육부 시민권국의 캐서린 라몬(Catherine Lhamon) 차관보는 “딥페이크로 인한 괴롭힘이 학교 환경에서 적대적인 분위기를 조성한다면, 이는 연방법에 따라 성차별로 간주될 수 있습니다. 학교는 성차별이 발생하지 않도록 신속하고 효과적인 조치를 취해야 합니다.” 라고 언급했다. 그러나 2025년 1월, 켄터키 연방지방법원은 해당 개정이 표현의 자유를 침해하고 교육부의 권한을 초과한다는 이유로 전국 효력 정지 판결을 내렸다. 이로 인해 현재는 2020년의 기존 Title IX 규정이 다시 적용되고 있는 상황이다. 법적 효력이 일시 정지된 가운데, 교육계와 민간기관들은 공백을 메우기 위해 자율적인 예방 교육에 박차를 가하고 있다.

4. 딥페이크 예방 교육 프로그램

가. Common Sense Education

Common Sense Education은 미국 내 90,000개 이상의 학교에서 채택되어 활용 중인 비영리 교육 프로그램으로, 디지털 시민성 교육을 중심으로 학생들에게 온라인 프라이버시, 딥페이크 식별법, 정보 검증 능력을 가르친다. 하버드 교육대학원(Project Zero)과 협력하여 개발된 이 커리큘럼은 다음의 여섯 가지 핵심 주제를 포함한다(*미디어 균형 및 웰빙, 디지털 발자국 및 정체성, 프라이버시 및 보안, 관계 및 커뮤니케이션, 사이버 괴롭힘 및 디지털 드라마, 뉴스 및 미디어 리터러시*) 또한, 딥페이크 대응을 위한 수업 모듈도 운영하고 있다.


common sense education

Read Laterally for Accuracy

NAME

Part 2 Directions: Hoax or Real?

Select one of the videos below. Using lateral reading, determine whether the video is a hoax. Using the chart below, provide corroboration from trustworthy resources you can find. (This means you might not record every source you look at.) Be sure to avoid ads, sponsored links and opinion pieces in your lateral reading. If you're in a group, each group member can select a different resource to explore.

Choose One:

Video 1 — Watch: "Snowboarder Girl Chased by Bear"

Resource Notes
- Fake video that shows a bear chasing a girl as she snowboards.
- This video is on YouTube, which some schools and local authorities block students from accessing.

Video 2 — Watch: "Loggers Couldn't Believe What They Found in the Middle of a Tree!"

- True video of a mummified dog found in a tree by loggers.
- This video is on YouTube, which some schools and local authorities block students from accessing.

Video 3 — Watch: "Proven Turmeric Cure Cancer"

- This questionable video presents the unsubstantiated health benefits of turmeric.
- This video is on YouTube, which some schools and local authorities block students from accessing.

common sense education

Read Laterally for Accuracy

NAME

The video I investigated: _____

Corroborating Source (link or citation)	Evidence (1-2 bullets of how the source validates or debunks)
video 1 is fake	• Snopes - "Snowboarder Girl" Chased By Bear • Global News - Video of Snowboarder Chased by Bear Was Part of a Viral Video "Social Experiment"
video 2 is real	• Newsweek - Strange Phenomenon Left Dog Stuck in Tree... • Snopes - Was This Dog Found 'Mummified' Inside the Trunk of a Tree?
video 3 presents unsubstantiated claims	• Mayo Clinic - Curcumin: Can It Slow Cancer Growth? • Cancer Research UK - Turmeric

I determine the information in the video is: ____ hoax ____ real because ...

[그림 1] Common Sense Education의 딥페이크 교육 자료

(1-1) Common Sense Education의 딥페이크 대응을 위한 수업 모듈

① Deepfakes and Democracy

딥페이크 기술이 민주주의에 미치는 영향을 탐구한다. 학생들은 딥페이크가 어떻게 허위 정보를 퍼뜨리고, 선거와 같은 민주적 과정에 영향을 줄 수 있는지에 대해 학습한다.

② Hoaxes and Fakes

학생들이 온라인에서 접할 수 있는 허위 정보와 딥페이크를 포함한 조작된 콘텐츠를 식별하는 방법을 가르친다. 학생들은 다양한 예시를 통해 진짜와 가짜 정보를 구분하는 기술을 습득한다.

③ Picture Perfect

이미지 조작의 개념을 소개하고, 딥페이크 기술이 어떻게 작동하는지를 이해하도록 돕는다. 학생들은 간단한 활동을 통해 이미지 조작의 윤리적 측면에 대해 생각해 볼 기회를 얻는다.

(1-2) 학년별 적용 예시

학년	적용 예시
초등학교 (K-5학년)	'Picture Perfect' 수업을 통해 이미지 조작의 기본 개념을 배우고, 온라인에서의 책임감 있는 행동에 대해 토론함
중학교 (6-8학년)	'Hoaxes and Fakes' 수업을 통해 딥페이크와 허위 정보를 식별하는 기술을 습득하고, 실제 사례를 분석함
고등학교 (9-12학년)	'Deepfakes and Democracy' 수업을 통해 딥페이크가 민주주의에 미치는 영향을 탐구하고, 비판적 사고 능력을 높임

나. Cyber Civics

Cyber Civics는 중학생을 대상으로 하는 3단계 교육 프로그램으로, 디지털 시민성, 정보 리터러시, 미디어 리터러시로 구성된다. 최근에는 딥페이크 기술의 위험성과 대응 전략을 포함한 모듈이 새롭게 추가되어, 허위 콘텐츠의 식별과 윤리적 대응 역량을 강화하고 있다. 미국 전역의 다양한 학교에서 채택되어 사용되고 있으며, 각 단계는 약 50분 길이의 주간 수업으로 구성된다.

단계	교육 프로그램
1단계	*1단계: 디지털 시민성 (Digital Citizenship)* - 기술이 사회에 미치는 영향과 디지털 도구의 사용에 대한 탐구 - 온라인에서의 시민의식과 책임 있는 행동에 대한 학습 - 디지털 평판 관리와 윤리적 사고를 통한 온라인 행동을 성찰 - 사이버 괴롭힘과 디지털 드라마에 대응하는 전략 학습 - 온라인 정체성과 개인정보 보호의 중요성 이해
2단계	*2단계: 정보 리터러시 (Information Literacy)* - 온라인에서 정보를 찾고, 평가하며, 활용하는 방법 학습 - 허위 정보와 선입견을 식별하고, 신뢰할 수 있는 정보를 구별하는 기술을 개발 - 디지털 도구를 활용하여 정보를 효과적으로 전달하는 방법 학습
3단계	*3단계: 미디어 리터러시 (Media Literacy)* - 미디어 메시지를 비판적으로 분석하고, 다양한 관점을 이해 - 창의적 미디어 콘텐츠 제작 및 윤리적 미디어 소비 습관 형성 - 디지털 플랫폼에서의 긍정적인 참여와 책임 있는 행동 실천

다. FBI Safe Online Surfing (SOS) Internet Challenge

FBI가 운영하는 SOS 프로그램은 3학년부터 8학년 학생들을 대상으로 온라인 보안, 사이버 괴롭힘 대응, 딥페이크 구별 방법 등 디지털 안전 전반에 대해 교육하는 무료 프로그램이다. 전국 학교 단위로 등록할 수 있으며, FBI 인증서를 수여하는 등 참여율을 높이는 방식으로 운영되고 있다.

라. Uncovering Deep-fakes: Classroom Guide

Uncovering Deepfakes

Appropriate for Grades 8+

AI for Education

Classroom Guide + Discussion Questions

Since 2019, the presence of **Deepfakes** – hyperrealistic AI-generated video, photo, and audio forgeries – has surged by 550%, reaching a staggering 95,820 documented deepfake videos in 2023 alone.

This blurring of reality requires a new approach to vetting if online content is real or fake. This guide is designed to build student awareness of the presence and impact of deepfakes, while providing key discussion topics on the ethics of AI-generated content.

What are Deepfakes?

Deepfakes are videos, photos, or audio recordings that use artificial intelligence to make it look or sound like someone is saying or doing something that is not real.

Deepfake Techniques

- **Face Swapping:** Replacing a person's face with another in a video or photo using AI.
- **Voice Cloning:** Using AI to mimic someone's voice.
- **Lip Syncing:** Making a person's lips appear to match different audio using AI.

The Dangers of Deepfakes

While deepfakes can be used for harmless or even educational purposes, they can also be used unethically in the following ways:

- **Identity theft:** Deepfakes can impersonate individuals in videos or audio recordings, potentially allowing criminals to commit fraud under someone else's name.
- **Threats/Blackmail:** Deepfakes can create convincing footage or audio that puts the subject in a bad light, which can then be used to threaten or blackmail them.
- **Cyberbullying:** Deepfakes can be used to create embarrassing or hurtful videos or audio recordings of someone.
- **Propaganda/Fake news:** Deepfakes can be used to create fake videos or audio recordings that trick people and sway their opinions on important topics.
- **Election manipulation:** Deepfakes can be used to make candidates look bad or confuse voters by creating fake speeches or interviews.
- **Nonconsensual Intimate Images (NCII):** Deepfake photos and videos that remove the subject's clothing without their knowledge or consent.

aiforeducation.io

[그림 2] AI for Education 교육 자료

AI for Education는 민간 교육 전문 기관으로, 정부나 공공기관이 아닌 비영리 조직이다. 이 기관은 학교와 교사들이 생성형 AI를 교육 현장에 책임감 있게 도입하고 활용할 수 있도록 지원한다. 주요 활동으로는 AI 리터러시 교육, 정책 개발, 커리큘럼 설계, 워크숍 제공 등이 있으며, 뉴욕시 교육청(NYC DOE), 휴스턴 교육구, 시카고 공립학교 등 150개 이상의 교육기관과 협력하고 있다. "Uncovering Deepfakes: Classroom Guide"는 중·고등학생을 대상으로 딥페이크의 개념, 위험성, 식별 방법, 윤리적 고려 사항 등을 다루는 수업 자료이다. 특히, 실제 사례를 기반으로 한 토론 주제를 통해 학생들의 비판적 사고와 윤리적 판단 능력을 키운다. 이 가이드는 학생들이 딥페이크 기술의 복잡성과 그로 인한 사회적, 윤리적 문제를 이해하고, 책임감 있는 디지털 시민으로 성장할 수 있도록 돕는다.

주요 토론 주제
비동의 딥페이크 이미지 : 한국 정부가 텔레그램에서 비동의 딥페이크 이미지 생성 봇의 확산에 대해 조사한 사례를 통해, 이러한 콘텐츠의 사회적·윤리적 함의를 탐구함
청소년 대상 딥페이크 범죄 : 뉴저지주의 청소년들이 동급생의 딥페이크 음란물을 생성·유포한 사건을 통해, 피해자의 심리적 영향과 법적 대응 방안을 토론함
권위자 사칭 : 메릴랜드주의 한 고등학교 교장이 딥페이크 음성 파일로 인해 인종차별 발언을 한 것으로 오해받은 사례를 통해, 딥페이크가 조직 내 신뢰에 미치는 영향을 분석함
딥페이크의 사회적 영향 : 딥페이크 기술의 발전이 온라인 상에서의 신뢰와 상호작용에 어떤 변화를 가져오는지에 대해 학생들의 경험과 의견을 공유함
딥페이크의 규제 필요성 : 딥페이크 기술의 사용을 금지해야 하는지에 대한 찬반 토론을 통해, 기술의 자유로운 발전과 사회적 안전 사이의 균형을 모색함
딥페이크의 긍정적 활용 : 교육·예술에서 딥페이크 기술의 윤리적 활용 방안을 탐색함
사회적 대응 전략 : 딥페이크 기술의 발전에 대비하여 개인, 교육자, 정책입안자, 기술 기업이 어떤 역할을 수행해야 하는지에 대해 논의함

마. Olweus Bullying Prevention Program (OBPP)

OBPP는 노르웨이 심리학자 댄 올베우스(Dan Olweus)가 개발한 학교폭력 예방 프로그램으로, 미국에서는 디지털 환경에서의 새로운 형태의 괴롭힘, 특히 딥페이크를 수단으로 한 정서적 폭력에 대응하는 기반 체계로 활용되고 있다. 이는 학교, 교실, 개인, 지역사회 수준에서 통합적으로 폭력과 따돌림을 줄이고 학생 간 긍정적인 관계를 촉진한다. 딥페이크 기반 괴롭힘 사례가 증가하면서, 일부 미국 학교들은 OBPP 체계를 확장해 조작 이미지 및 AI 기반 허위 콘텐츠를 통한 괴롭힘도 보고 체계에 포함하고 있다. 펜실베이니아주의 Inglewood 초등학교는 OBPP에 기반해 디지털 이미지 조작도 괴롭힘 행위로 분류하고 교육과 개입을 진행 중이다.

학교 수준	괴롭힘 예방 위원회 구성, 교직원 교육, 학부모 참여
교실 수준	정기적 회의와 또래 간 역할극, 공감 능력 강화 활동
개인 수준	가해자·피해자 맞춤 개입과 상담
지역사회 수준	지역사회와 협력해 예방 메시지 확산

5. 맺음말

AI 기술의 발달은 교육현장에 다양한 기회를 제공하는 동시에 새로운 위험도 동반하고 있다. 딥페이크 범죄는 학생들의 인권과 안전을 침해할 수 있는 위협으로, 이를 예방하기 위한 제도적 노력과 교육현장의 대응이 병행되어야 한다. 미국의 사례는 우리에게도 중요한 시사점을 제공하며, 국내 역시 AI 기술의 윤리적 사용과 학생 보호를 위한 디지털 리터러시 교육 강화가 필요한 시점이다.

【참고 자료】

- https://www.nytimes.com/2024/04/08/technology/deepfake-ai-nudes-westfield-high-school.html
- The Lancaster County District Attorney's Office, https://lancaster.crimewatchpa.com/da/11617/post/2-juveniles-charged-connection-ai-generated-images-lancaster-country-day-school-students?
- The U.S. Department of Education's New Title IX Rules, https://19thnews.org/2024/04/biden-administration-new-title-ix-regulations/
- FBI, https://www.fbi.gov/how-we-can-help-you/outreach/safe-online-surfing-sos-program
- Havard Graduate School of Education's Project Zero, https://pz.harvard.edu/resources/digital-literacy-and-citizenship-curriculum
- CSE, https://hwb.gov.wales/api/storage/22510c85-b110-4e69-acd7-051bc478124e/10.6%20-%20Read%20Laterally%20for%20Accuracy%20Handout%20(teacher%20version)%20-%20English.pdf?preview=true
- AI For Education, https://www.aiforeducation.io/ai-resources/uncovering-deepfakes
- Cybercivics, https://www.cybercivics.com/about

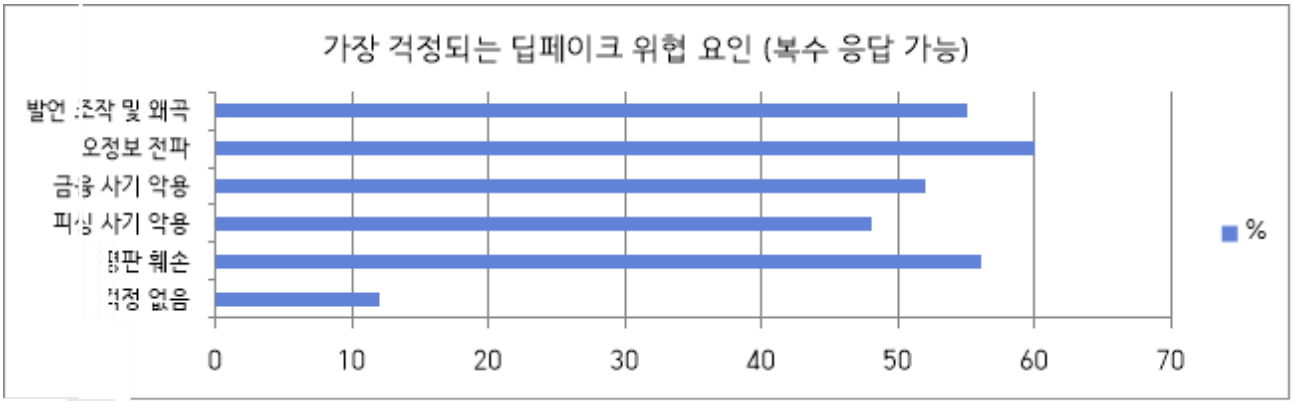
캐나다의 딥페이크 등 디지털 범죄 예방 교육

발간위원 : 안예린(포항송곡초등학교 교사)

AI의 발전으로 전세계 곳곳에서 인공지능 기반 기술을 이용한 디지털 범죄가 사회 전반에 큰 위협이 되고 있다. 특히, 머신러닝과 AI 기술로 인간의 목소리, 행동 등을 조작해 만든 딥페이크 관련 범죄가 큰 화두에 올랐다.

토론토 메트로폴리탄 대학의 연구에 따르면, 캐나다인의 60% 이상이 이미지, 비디오, 오디오 등 어떤 형식으로든 딥페이크를 경험한 적이 있다고 응답했다. 다른 국제 조사[8]에서도 딥페이크에 대해 “자라나는 걱정거리, 온라인 정보의 신뢰성 저해, 유해함” 등 부정적인 응답이 60~80%에 육박한 것에 비해 “일시적인 기술 트렌드, 피해 가능성 없음” 등 상대적으로 긍정적인 응답은 비율은 10% 이하였다. 또한 딥페이크가 일상 생활에 초래할 위협 요인에 대한 캐나다인들의 공감대도 넓었다.

〈표 1〉 캐나다인의 딥페이크 인식 중 딥페이크가 초래할 위협 요인



캐나다 전역에서 심화하는 우려와 딥페이크 기술의 악용 가능성을 염려하여 캐나다 정부는 딥페

8) iProov: Deepfake Statistics & Solutions | How To Protect Against Deepfakes

이크를 필두로 한 여러 디지털 범죄를 시급히 해결해야 할 사이버 위협 과제로 설정하였다.

실제로 캐나다에서도 초, 중, 고 연령대 아동(이하 K-12)이 연루된 여러 딥페이크 범죄 사건이 발생하였으며, 피해 대상과 범죄 유형도 점점 다양화되고 있어 교육 주체들의 적극적인 개입에 관한 논의가 진행되고 있다. 이에 본 기사는 캐나다 K-12 교육 현장에서의 디지털 범죄, 특히 딥페이크 관련 동향과 대응 현황을 다룬다.

1. 캐나다의 디지털 성범죄 경향 및 사례

가. 캐나다의 디지털 성범죄 경향

2024년의 국제 조사[9]에 따르면, 캐나다 대학생의 80퍼센트 이상이 성적 댓글, 성희롱성 이메일과 메세지 수신 등 디지털 성범죄(Technology Facilitated Sexual Violence, TFSV) 피해 경험이 있다고 응답했다.

캐나다 내부에서도 남성보다는 여성이, 비장애인보다는 장애인이, 백인보다는 흑인·무슬림과 같이 소외된 인종이나 민족적 배경을 가진 학생들의 디지털 성범죄 피해율이 높았다. 또한 성소수자 학생들은 중증도의 디지털 성범죄를 경험하는 경우가 많았다. 이에 대하여 조사 보고서에서는 디지털 성범죄 피해 경험 확률이 학생들의 문화·인종·성적 소수자 정체성이 아닌, 소수자 개인이 겪는 시스템적 불평등에 기인함을 명시하고 있다.

캐나다에서 미성년자의 성적 사진은 딥페이크 여부와 상관없이 아동 음란물로 처벌된다. 캐나다 내부에서 운영 중인 온라인 사이트들과 SNS 플랫폼도 자사 사이트에서 발견한 미성년자들의 음란 사진들을 경찰에 신고하여 처리하고 있다. 그러나 AI 기술의 발달로 딥페이크의 사실성이 높아지고 제작이 용이해짐에 따라 딥페이크 범죄 피해 범위와 양상은 더 악화될 예정이다.

나. 캐나다 학교에서의 딥페이크 관련 피해 사례와 신고 기관

2024년 11월, 캐나다 토론토의 16세 고등학생 Ruby는 본인의 13세 시기 사진을 기반으로 한 딥페이크 누드 이미지가 온라인에 유포된 사실을 알게 되었다. 익명의 메시지로 해당 사이트 주소를 받은 뒤 피해를 인지한 Ruby와 그녀의 부모는 Cybertip.ca에 피해 사실을 바로 신고했다. Cybertip.ca는 아동 대상 온라인 성 착취 신고를 위한 캐나다 국가 직통 신고 전화 창구로, 작년 한 해 동안 Ruby의 사례와 유사한 딥페이크 성적 이미지 4,000건 이상을 처리했다고 밝혔다.

9) Technology-Facilitated Sexual Violence: Prevalence, Risk, and Resiliency in Undergraduate Students

2. 캐나다의 디지털 성범죄 연구 기구, DIY

DIY(Digitally Informed Youth, 디지털 교육을 받은 청소년)은 캐나다 전역의 디지털 성범죄를 조사하는 연구 프로젝트 기구이다. 2023년 DIY 기구는 캐나다의 성교육 위원회(Sex Information & Education Council of Canada, SIECCAN)와 연합해 진행한 디지털 안전 연구 프로젝트(Digital Safety research project)를 통해 캐나다 학교의 디지털 성범죄 대처를 분석·평가하였다. 그리고 분석 결과를 활용해 캐나다 전역의 중·고등학교가 청소년 연령대의 학생들을 위해 교육과정과 학교 정책 및 법률에서 디지털 성범죄를 다루는 방법을 설명하는 지침[10] 을 발표했다.

〈표 2〉 캐나다 학교의 디지털 성범죄 대처에 대한 평가

특징	SIECCAN과 DIY의 평가
일관성	디지털 성범죄에 대해 캐나다 전역에 걸쳐 일관적으로 대응하지 못해 교육 문서마다 상당한 차이가 발견된다.
포괄성	디지털 성범죄에 관한 교육이 교육법에서의 사이버 괴롭힘 방지, 혹은 교제 관계에서의 위험 주제에 한정되어 있다.
통합성	디지털 성범죄에 관한 교육이 중·고등학교 전 학년 과정에서 여러 교과를 통틀어 간학문적으로 이루어지지 않고 있다.
지원 접근성	디지털 성범죄에 대해 지원 방식과 도구가 아닌 위험 중심으로 접근해 학생에게 낙인을 찍거나 부끄러움을 느끼게 할 수 있다.
교차성	디지털 성범죄에 대한 교육이 교차성(학생 정체성의 복합적 작용)을 충분히 고려하지 못하고 있다.

더불어, 보고서에서는 각 주/준주마다 독립적인 교육부가 존재하는 캐나다의 상황을 반영. 주/준주별 디지털 성범죄 대처 현주소를 파악하기 위해 관련 내용의 교육과정 및 정책 · 공문 반영 현황을 제시하고 있다.

10) Technology-Facilitated Sexual Violence in Canadian Educational Curricula, Policies, and Legislation.

Table 1. *Educational Curricula across Provinces and Territories.*

Curriculum Features	AB	BC	MB	NB	NL	NS	NV	NWT	ON	PEI	QC	SK	YK
Addresses gender-based harm		✓	✓	✓*		✓			✓				✓
Addresses sexuality-based harm		✓	✓	✓*					✓		✓		✓
Discusses abuse/ relationship violence/ sexual violence	✓	✓	✓	✓*		✓			✓	✓	✓	✓	✓
Recognizes that sexual violence can occur online		✓							✓				✓
Includes content on (cyber)bullying and/ or TFSV-specific online behaviours (e.g., sexting, dissemination of intimate content)		✓	✓			✓	✓	✓	✓	✓		✓	✓
Addresses legal consequences of online behaviour		✓*							✓	✓			
Addresses digital etiquette/ethics	✓*	✓	✓	✓	✓	✓		✓	✓	✓		✓	✓
Discusses general healthy relationship skills	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Addresses power imbalances		✓	✓	✓	✓				✓	✓			✓
Discusses intersectionality			✓*	✓*									

*Note: these concepts are discussed in suggested/external teacher resources, not formalized in the curricula.

Table 2. *Policies and Other Government Documents across Provinces and Territories.*

Policy Features	AB	BC	MB	NB	NL	NS	NV	NWT	ON	PEI	QC	SK	YK
Addresses gender-based violence			✓						✓		✓		
Addresses sexuality-based violence									✓		✓		
Recognizes that TFSV is sexual in nature	✓		✓	✓	✓	✓			✓	✓	✓	✓	✓
Recognizes that TFSV occurs both online and offline	✓	✓	✓	✓	✓	✓		✓	✓	✓	✓	✓	
Acts/policies recommend consequences/processes to address TFSV		✓	✓		✓	✓	✓		✓		✓		
Recognizes power imbalances			✓		✓				✓		✓	✓	
Discusses responsibility to report	✓		✓			✓			✓				
Identifies action plan/ prevention strategy			✓	✓	✓	✓		✓			✓	✓	
Policy emphasizes, stipulates, and/or guides school codes of conduct		✓	✓	✓		✓		✓					

[그림 1, 2] 캐나다 내 지역별 디지털 성범죄 관련 내용 교육과정 및 정책 · 공문 반영 현황

〈표 3〉 캐나다 내 지역별 디지털 성범죄 관련 교육과정 및 교육 정책 평가 항목

교육과정	교육 정책
젠더(gender) 기반 피해를 다루는가?	젠더(gender) 기반 폭력을 다루는가?
성적 지향(sexuality) 기반 피해를 다루는가?	성적 지향(sexuality) 기반 폭력을 다루는가?
학대·연인 관계 내 폭력·성폭력에 대해 논의하는가?	디지털 성범죄의 성적인 특성을 인식하고 있는가?
성폭력이 온라인 환경에서도 발생할 수 있음을 인식하고 있는가?	디지털 성범죄를 다루기 위한 결과/방법론적 법안 ·정책을 권장하고 있는가?
사이버 괴롭힘이나 디지털 성범죄 관련 온라인 행위(성적 대화, 사적 이미지 유포 등)에 대한 내용을 포함하고 있는가?	권력 불균형을 인식하고 있는가?
온라인에서의 행동에 대한 법적 결과를 다루고 있는가?	신고 책임에 대해 논의하고 있는가?
디지털 예절·윤리를 다루고 있는가?	디지털 성범죄 예방 및 계획 전략을 제시하는가?
건강한 관계를 위한 전반적인 기술을 다루고 있는가?	학교 규율이나 행동 강령을 강조·안내하는 정책이 있는가?
권력 불균형을 인식하고 있는가?	–

*교육과정 평가 항목은 정규 교육과정이 아닌 참고용 · 외부 교육 자료를 대상으로 함.

또한 보고서는 교육 현장 인력, 교육청, 정책 입안자들이 교육과정을 개선하고 정책을 발전시키는 데 활용할 수 있는 권고안도 제시한다. 특히 디지털 성범죄에 대한 교육과 법적 대응 능력이 부족한 지역의 교육청이 해당 능력을 개발하고, 중·고등학생들의 정보 기술 사용 경험과 온라인·오프라인 피해에 대해 교육하기 위하여 고려할 사항은 아래와 같다.

〈표 4〉 디지털 성범죄 대응 능력을 높이기 위한 교육과정·정책 개선 방향

특징	개선 방향
구체성	교육과정과 정책에 다양한 형태의 디지털 성범죄를 명확히 구분해 반영하고, 단순 사이버 괴롭힘 이상의 구체적인 내용을 포함해야 한다.
통합성	온라인과 오프라인 경험을 구분하지 않고, 학생들의 실제 삶 속에서 디지털 성범죄가 일어나는 맥락을 모두 반영해야 한다.
무해성	디지털 성범죄에 대한 교육이 수치심이나 공포를 일으키는 방향이 아니라 비판적 사고 중심으로 이뤄져야 한다.
권리 인식·지원	학생들에게 디지털 기술 관련 권리와 책임에 대해 교육하고 디지털 성범죄 노출 시 이용 가능한 자원 및 지원체계를 명확히 알려야 한다.
포용성	성별, 성적 지향에 따라 디지털 성범죄의 피해 정도가 다름을 인식하고, 이런 차이를 반영해 교육적 접근을 다양화해야 한다.
교차성	인종적 배경, 정체성 등 다양한 요인이 디지털 성범죄에 미치는 영향을 다루고, 교차적 차별 경험을 반영해 교육을 실시한다.

3. 주/준주별 교육 현장에서의 디지털 성범죄 대응 노력

가. 브리티시 컬럼비아, BC

BC주의 교육과정은 개념 중심으로 구성된다. 디지털 성범죄 관련 개념에는 건강한 관계, 기술 윤리, 디지털 시민성 등이 있으며 사이버 괴롭힘을 중심으로 교육 정책 수준에 명시되었다.

학년	과목	디지털 성범죄 관련 내용
9학년	신체 및 건강 교육	건강한 관계, 차별·괴롭힘 대응 전략
10학년	신체 및 건강 교육	9학년과 동일한 내용 반복 학습
	컴퓨터	기술 사용의 영향, 기술 윤리, 디지털 리터러시와 시민성
11학년	인간·가족 관계	관계 내 의사소통, 위험한 관계에 대한 인식과 대처
	디지털 의사소통	디지털 소통 윤리·위험·법적 문제, 디지털 리터러시
12학년	컴퓨터 정보 시스템	디지털 보안 위험 및 적절한 정보 통신 기술 사용

나. 온타리오

온타리오주에서는 관련 주제를 보건, 기술, 컴퓨터 과목에서 다루며 사이버 괴롭힘과 성희롱 중심으로 교육 및 정책에 반영하고 있다. 주 교육과정에는 관계, 의사소통, 안전한 기술 사용, 윤리 등이 포함되어 있으며 교육법 개정을 통한 예방 및 대응 지침 마련 또한 강조하고 있다.

학년	과목	디지털 성범죄 관련 내용
9학년	건강하고 활동적인 삶(HALE)	전자 소통 기술 사용, 사이버 안전 전략, 건강한 관계
10학년	HALE, 컴퓨터	성적 의사결정·소통 기술, 컴퓨터 관련 윤리·법적 이슈
11학년	HALE, 컴퓨터, 컴퓨터 기술	스트레스 상황 대처, 인터넷 안전, 사생활·권리 침해
12학년	HALE, 컴퓨터, 컴퓨터 기술	관계 속 폭력 인식·대응, 사이버 위험 요소, 컴퓨터 윤리

다. 퀘벡

퀘벡주에서는 관련 주제를 성교육과 윤리교육을 통해 다루며 관계 내 폭력, 성폭력, 사이버 괴롭힘 등을 중심으로 학생들의 비판적 사고와 책임감을 기르는데 목표를 두고 있다. 사이버 괴롭힘으로 대표되는 디지털 성범죄를 폭력으로 정의하고, 관련 대응 계획도 마련되어 있다.

학년	과목	디지털 성범죄 관련 내용
7~8학년	성교육, 윤리 및 종교·문화	교제 관계 성찰, 성폭력, 성 가치와 사회규범의 변화 등
9학년	성교육	관계 내 갈등 해결 전략, 폭력 인식
10학년	성교육	폭력 징후 인식과 대처
11학년	성교육	관계와 성폭력 연계 심화 학습

4. 맺음말 및 시사점

캐나다 교육계는 딥페이크를 필두로 한 디지털 범죄의 심각성에 경각심을 가지고 연구기관과 협력하여 각 주/준주 교육부의 디지털 성범죄 대응 현황을 분석, 전국적인 개선 지침을 제공하는 등 적극적으로 대응하고 있다. 더불어 모범적인 다문화 국가 캐나다답게 문화·인종·성적 소수자 배경 학생들의 피해에도 주의를 기울이는 모습은 대한민국 교육계에도 중요한 메세지를 던진다.

【참고 자료】

- https://theconversation.com/canadian-schools-need-to-address-digital-sexual-violence-in-their-curricula-and-policies-220633
- https://www.cbc.ca/news/canada/deepfake-minors-porn-explicit-images-1.7385099

호주와 뉴질랜드의 딥페이크 등 디지털 범죄 예방 교육

발간위원 : 최지원(상대초등학교 교사)

1. 호주의 디지털 범죄 예방 교육

가. 최근 호주의 디지털 범죄 관련 대응 양상

2024년 6월 마크 드레퓌스 호주 법무장관은 딥페이크 성착취물 제작 및 유포를 처벌하는 형법 개정안을 발표하였다. 구체적으로는 상대방의 동의 없이 딥페이크 음란물을 제작할 경우 최고 징역 7년형에, 해당 이미지 등을 동의 없이 유포할 경우 최고 징역 6년형에 처한다는 내용이다.[11)]

이후, 같은 해 11월 호주 의회에서는 16세 미만 청소년의 SNS 이용을 전면 금지하는 법안을 통과시켰다. 이 법안은 SNS 중독 및 무분별한 사용으로 인한 딥페이크, 스토킹 범죄 등 피해로부터 청소년을 보호하기 위하여 제정되었으며, 16세 미만 아동 및 청소년이 SNS에 계정을 생성하고 이용할 경우 해당 플랫폼에 최대 5,000만 호주달러(한화 약 450억원)의 벌금을 부과한다는 내용이다.[12)] 이 법안은 SNS 이용 가능 연령을 16세 이상으로 가장 높게 규정한 점, 부모의 동의와 상관없이 모든 미성년자의 SNS 이용을 제한한다는 점 등 세계 각국에 비해 강력한 규제를 특징으로 한다. 이 법안은 2025년 1월부터 1년간의 도입기를 거쳐 본격 시행될 전망이다.

이처럼 호주에서는 디지털 범죄와 관련하여 매우 강력하게 단속하겠다는 입장을 취하고 있으며, 국가적 차원에서 아동 및 청소년, 그리고 성인에 이르기까지 모든 자국민을 디지털 범죄로부터 보호하고 범죄를 예방하기 위하여 총력을 기울이고 있다. 이에 호주 교육당국에서는 학교에서 디지털 범죄 예방 교육이 활발하게 이루어질 수 있도록 다방면으로 학교와 교사를 지원하고 있다.

11) BBC news Korea(https://www.bbc.com/korean/articles/c80l810e1jno)
12)SBS news Korea(https://www.sbs.com.au/language/korean/ko/article/people-who-share-explicit-deep-fake-imagery-will-face-up-to-seven-years-in-prison/7ti9p2gdf)

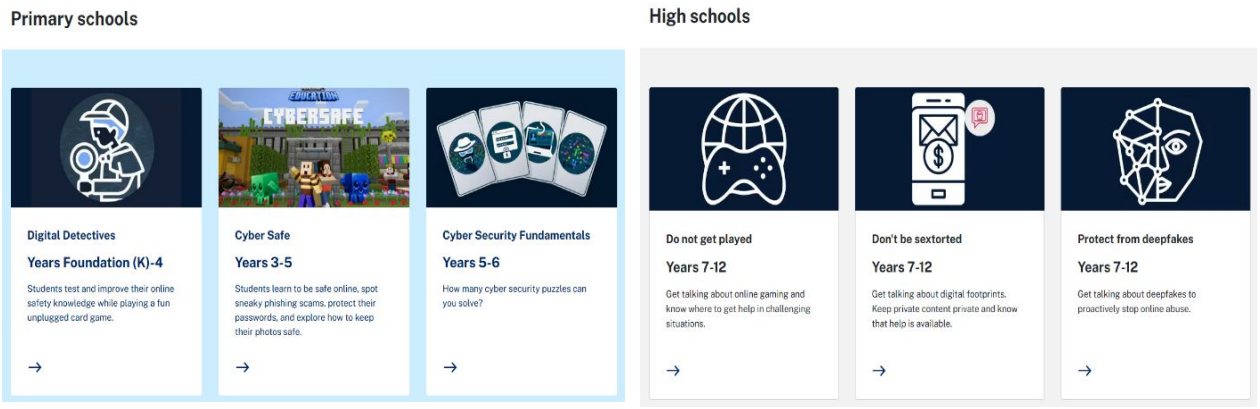
나. 호주의 디지털 범죄 예방 교육

호주 뉴사우스웨일스주 교육부에서는 디지털 시민권(digital citizenship) 교육을 통해 학생들이 바람직한 디지털 시민의식을 함양하도록 하고 있다. 이와 관련하여 디지털 시민권 웹사이트를 별도 운영하면서 학생, 교사, 학부모에게 안전하고 윤리적인 온라인 행동에 대한 실질적인 조언을 제공하고 있다. 해당 웹사이트에서는 다양한 수업 계획과 자료들을 신뢰할 만한 출처로부터 수집하여 제공함으로써 교실수업에 그대로 활용할 수 있도록 하고 있다.

1) Cybermarvel 사이버 안전 교실

뉴사우스웨일스주 소속 교사들은 누구나 교육부의 Universal Resources Hub에서 제공하는 사이버마블(Cybermarvel)의 사이버 안전 교실[13]을 이용할 수 있다. 여기에는 가상 교실, 비디오 및 팟캐스트, 게임, 오프라인 수업 등을 지원하는 다양한 자료가 탑재되어 있다. 특히 인상적인 자료는 사이버 안전교육 내용을 '마인크래프트(Minecraft)'와 같은 전 세계 청소년들이 즐겨 하는 게임을 통해 구현한 것이다. 교사라면 누구나 이 자료에 손쉽게 접근하여 교실수업에 활용할 수 있도록 했다는 점에서 자료의 유용성이 높아 보였으며, 학생들이 흥미를 가지고 수업에 참여할 수 있도록 하는 동기유발 소재이자 수업활동 자료로써 효과성이 분명하였다.

사이버 안전 교실의 자료들은 초등학교와 고등학교로 학교 수준에 따라 나누어 제공되고 있으며, 수준에 따라 학습의 범위와 차시, 주제의 심도 등이 다르게 구성되어 있는 것을 확인할 수 있다. 또한 사이버 안전 교실에는 수업 대상이 되는 학생들의 학년에 따라 자료를 구분하여 제시하고 있어 교사들이 학년성에 적합한 수업 자료를 가지고 수업을 계획 및 실행할 수 있도록 지원하고 있다.



[그림 1] 사이버 안전 교실에서 제공하는 수업 자료 일부(좌: 초등학교용, 우: 고등학교용)

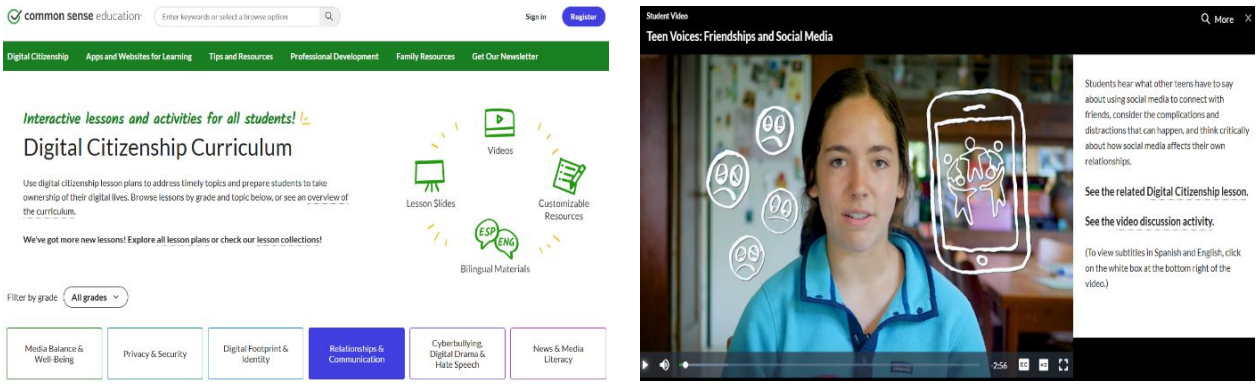
13) [그림 1] 이외의 더욱 다양한 수업 자료 예시는 뉴사우스웨일스주 교육부 홈페이지에서 추가적으로 확인할 수 있다 (https://www.nsw.gov.au/education-and-training/cybermarvel/cyber-safe-classroom).

<표 1> Cybermarvel의 온라인 수업 계획

수준	단계	제목	내용
초등	2	온라인 안전 실천 (Be safe online)	영상, 동료 토론, 학생 중심 과제를 활용하여 온라인 안전과 관련된 주제를 탐구하는 활동
	3	온라인에서 친절하게 대하기 (Be kind online)	사이버 괴롭힘의 징후를 학습하고 토론하며, 그것을 목격하거나 경험했을 때 자신의 감정을 탐구하는 활동
		디지털 탐정이 되어 보세요 (Be a digital detective)	온라인 정보를 비판적으로 평가하여 정보에 기반한 결정을 내리고, 책임감 있게 공유하는 방법을 배우는 활동
고등	4	디지털 리더 되기 (Be a digital leader)	온라인 콘텐츠 제작 과정과 사용, 온라인 자료의 활용과 출처 진위 여부에 대한 판단 능력을 기르는 활동
	5	강력한 디지털 시민이 되세요 (Be an empowered digital citizen)	항상 옳은 답이나 그른 답이 있는 것이 아닌 온라인 시나리오를 읽고 상황을 헤쳐 나가는 연습 활동

2) Common Sense 디지털 시민권 교육과정

뉴사우스웨일스주 교육부는 유치원부터 12학년까지의 학생들을 대상으로 계획된 디지털 시민권 교육과정 정보를 제공하고 있다. 여기에서는 디지털 시민권 교육과정 개요와 더불어 학년별 및 주제별 수업 사례를 확인할 수 있다. 해당 교육과정은 미디어 균형과 웰빙, 개인정보 보호 및 보안, 디지털 발자국과 정체성, 관계 및 커뮤니케이션, 사이버 괴롭힘, 디지털 드라마 및 증오 표현, 뉴스 및 미디어 리터러시 등 6개의 핵심 주제를 가지고 설계되었다.



[그림 2] 디지털 시민권 교육과정(좌)과 수업 사례(우, 7학년 'My social media life')

특히 Common Sense Education에서는 학생들의 학습에 사용할 수 있는 어플리케이션과 웹사이트를 엄선하여 그 목록을 제공하고 있으며, 디지털 시민권뿐만 아니라 생성형 AI와 관련하여 수업 내외에서 활용 가능한 도서, 팟캐스트, 영화 등 다양한 멀티미디어 자료를 소개하고 있다. 또한 교사 연수 자료와 학부모 워크숍 자료, 가정에서 가족이 함께 활용할 수 있는 자료 등을 제공하여 가정과의 연계를 통한 디지털 시민의식 교육을 진행하고 있다.

[그림 3] 디지털 시민권 학부모 워크숍 자료

2. 뉴질랜드의 디지털 범죄 예방 교육

가. 뉴질랜드의 청소년 디지털 범죄 현황

뉴질랜드 역시 청소년들이 디지털 범죄에 연루되고 있는 현실에서 자유롭지 못하다. 청소년들 사이에서 AI를 이용한 온라인 괴롭힘의 한 형태로 교실 내외에서 시시각각 일어나고 있다. 2015년 유해 디지털 통신법(Harmful Digital Communication Act)이 제정되어 시행되고 있음에도 불구하고, 해당 법에서는 온라인에서의 학대, 협박, 괴롭힘 등에 사용되는 이미지가 사실적인 것인지 혹은 인위적으로 만들어낸 것도 해당되는지 등에 관해 명확하게 규정하고 있지 않아 딥페이크 범죄로부터 실질적인 법적 보호가 이루어지기 힘든 실정이라는 것이 일각의 보도이다.[2)]

한편, 뉴질랜드 정부에서는 인터넷 감시 재단(Internet Watch Foundation)을 통해 하루에 최대 30,000개의 유해 사이트를 차단하고 삭제하는 활동을 이어가고 있다. 이에 대해 메이크스 센스(Makes Sense, 뉴질랜드 어린이를 위한 안전한 디지털 공간을 옹호하는 단체)는 시시각각 새롭게 만들어지는 딥페이크 이미지 및 영상을 완전히 막기에는 부족하다는 의견을 밝히면서 뉴질랜드의 온라인 유해 성적 콘텐츠 규제가 다른 나라에 비해 뒤처져 있음을 지적했다.

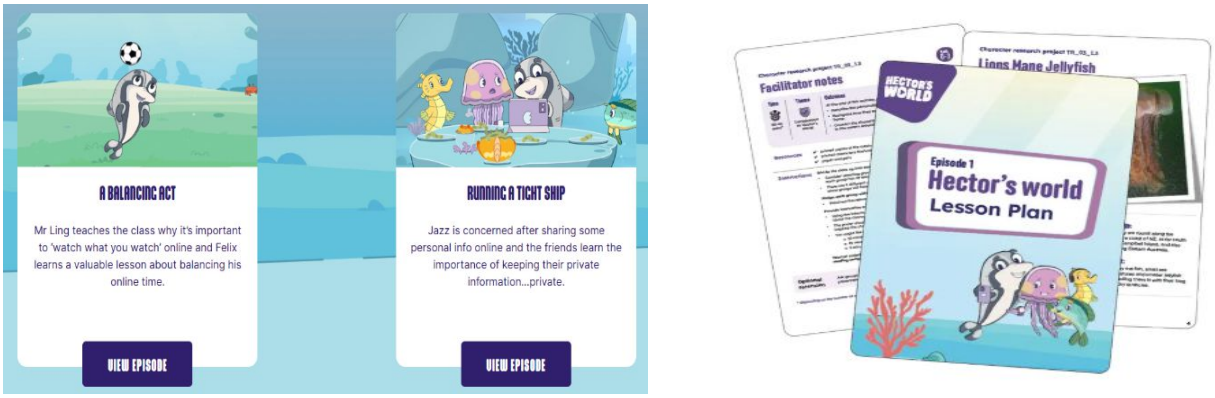
이와 같은 기존의 기술적·법적 안전장치의 한계를 극복하고 더욱 다층적인 대응 전략을 제안하기 위해 2024년 12월 뉴질랜드 넷세이프(Netsafe)와 AIAPI(AI Asia Pacific Institute, AI 아시아태평양기구)가 함께 뉴질랜드 내 온라인 안전 거버넌스 체계 강화를 위한 'AI와 온라인 안전: 새로운 위험과 기회(Discussion Paper on AI and Online Safety: Emerging Risks and Opportunities)' 리포트를 발간했다. 현재 뉴질랜드에서는 해당 리포트에서 구체적으로 제시하고 있는 정책 과제를 심도 있게 검토하고 책임 있는 생성형 AI 거버넌스 모델 구축을 위해 노력하고 있다.

나. 뉴질랜드의 디지털 범죄 예방 교육

뉴질랜드에서 학교 디지털 범죄 예방 교육을 지원하는 기관은 넷세이프(Netsafe)와 케테(Kete)가 대표적이다. 넷세이프는 비영리 온라인 안전 기관으로 온라인 안전에 관한 교육 및 컨설팅을 주관하고 있으며, 모든 연령을 대상으로 디지털 안전교육과 범죄 예방 교육을 실시하고 있다. 케테는 넷세이프에서 학교 온라인 안전교육을 지원하기 위해 별도 운영하는 자료 허브로, 교사와 학교 리더십을 위한 정책 가이드, 교실수업에서 사용할 수 있는 자료 등을 제공하고 있다.

1) 헥터의 세계(Hector's World)

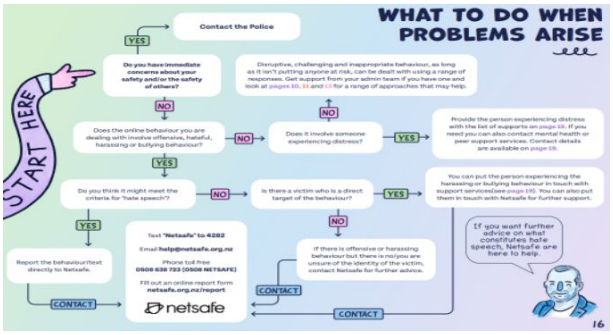
헥터의 세계는 5~10세 어린이를 대상으로 재미있고 유익한 애니메이션 에피소드를 통해 온라인 안전 수업을 제공하기 위해 만들어진 콘텐츠다. 모든 에피소드는 Youtube를 통해 누구나 이용할 수 있다. 전체 에피소드에 대한 대본을 함께 확인할 수 있으며, 영상 활용 수업 지도안, 교실과 가정에서 영상 시청 후 사용할 수 있는 활동지 등도 함께 제공하고 있다.



[그림 4] Hector's World 애니메이션 영상(좌)과 수업 자료(우)

2) 청소년 액션 스쿼드(Youth Action Squad)

청소년 액션 스쿼드는 또래 친구들의 온라인 안전과 웰빙에 관심이 있는 청소년들을 위한 프로그램이다. 청소년들은 그들만의 팀을 구성하여 다른 학생들에게 온라인 문제와 어려움에 대해 알리고 필요 시 지원하는 역할을 수행한다. 팀에는 교사가 반드시 함께 참여해야 하며, 학생들이 스스로 팀원을 모집하고 활동 계획을 수립한 후 한 학기에 최소 한 번의 행사를 진행한다. 청소년 액션 스쿼드를 통해 학생들은 디지털 시민의식에 관한 포스터 제작, 소그룹 활동, 토의토론, 학교 방송 출연 등 다양한 활동에 참여하면서 YAS 리더가 되어 또래 친구들을 지원하게 된다.



[그림 5] Youth Action Squad 활동 자료(좌), YAS 앰배서더 학생 인터뷰(우)

3. 맺음말

호주와 뉴질랜드의 디지털 범죄 예방 교육의 특징으로부터 다음과 같은 시사점을 발견할 수 있었다. 첫째, 디지털 시민의식 교육을 위한 별도의 교육과정을 개발하고 체계화하여 운영하고 있다는 점이다. 우리나라에서도 디지털 역량 교육을 의무로 실시하고 있으나, 그 수준과 내용, 방법 등을 단위학교에서 자체적으로 계획하여 추진하도록 하고 있어서 교육적 효과와 체계성을 확보하기에 어려움이 있다. 둘째, 디지털 범죄 예방 교육을 위한 자료 허브를 별도 운영하면서 방대한 자료를 모아 하나의 창구를 운영하고 있으며, 이를 지속적으로 업데이트함으로써 자료의 질을 관리하고 있다는 점이다. 우리나라에서도 이와 같이 할 경우, 현재 '함께학교', '에듀넷', '도란도란' 등에 산재하고 있는 디지털 역량 교육 자료들이 한 군데에 모이게 되므로 자료를 검색하고 수집하는 측면에서 접근성과 유용성을 높일 수 있을 것이다.

전 세계가 디지털 범죄와의 전쟁을 선포한 요즘, 디지털 범죄 예방 교육은 시의적 적합성이 분명하다. 두 나라의 사례를 반석 삼아 향후 우리나라의 디지털 범죄 예방 교육이 더욱 효과적으로 이루어질 수 있기를 기대해 본다.

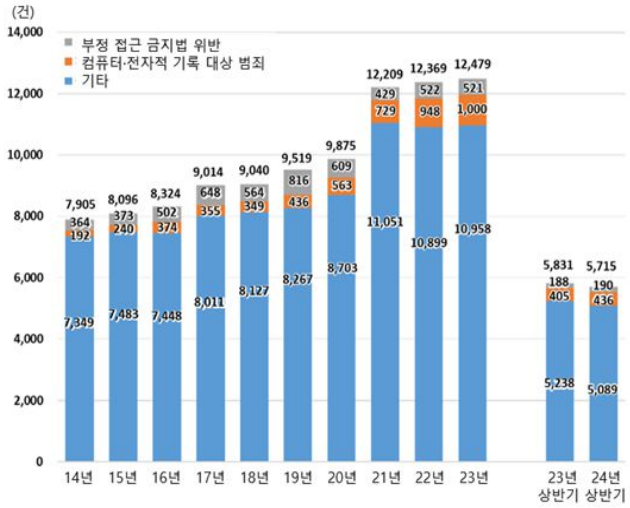
【참고 자료】

▶NSW Department of Education, 교사를 위한 디지털 시민권 수업 자료
https://www.nsw.gov.au/education-and-training/digital-citizenship?language=ko-KR
▶Austrailia eSafety Commissioner, Online safety 교사 연수 자료 및 수업 활용 가능 자료
https://www.esafety.gov.au/educators
▶AI Asia Pacific Institute, AI and Online Safety: Emerging Risks and Opportunities
https://aiasiapacific.org/our-work/ai-and-online-safety-emerging-risks-and-opportunities/
▶NETSAFE New zealand, https://netsafe.org.nz/
▶KETE New zealand, https://education.netsafe.org.nz/

일본의 딥페이크 등 디지털 범죄 예방 교육

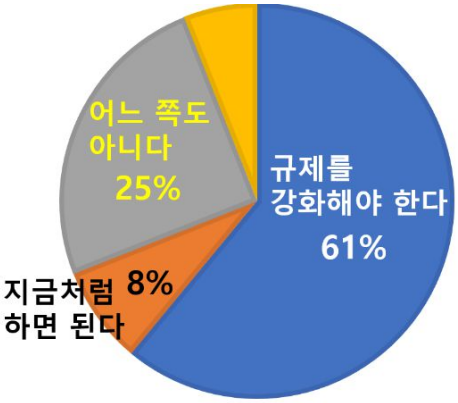
발간위원 : 최광현(복주초등학교 교사)

1. 일본의 디지털 범죄 현황



[그림 1] 사이버 범죄 검거 건수 추이 (출처: 일본 경찰청)

2024년 일본 경찰청 발표에 따르면 일본의 디지털 범죄는 피싱, 사이버 사기, 개인정보 침해, 랜섬웨어 공격, 청소년 범죄 등 다양한 형태로 나타나고 있으며 발생 건수 또한 점차 증가하는 추세이다. 특히 AI 기술 발달 상황과 맞물려 일본에서는 AI를 악용한 사이버 범죄 발생 또한 늘고 있는데, 생성형 AI를 사용해 만든 불법 프로그램을 배포하거나 이를 이용해 사이버 공격을 수행하는 사례, AI를 이용해 피싱 이메일과 가짜 정보를 생성하는 사례, AI를 이용해 수집된 데이터를 다크웹에서 판매하거나 악용하는 사례 등 기존에 없던 새로운 디지털 범죄 유형이 끊임없이 보고되고 있다.



[그림 2] '생성형 AI의 규제' 여론 조사 결과 (출처: NHK)

일본에는 아직 생성형 AI를 규제하는 법률이 제정되지 않은 상황이다. 하지만 딥페이크 영상이나 이미지 등으로 인해 문제가 발생하는 사례를 비롯해 생성형 AI를 이용한 디지털 범죄가 지속적으로 늘고 있는 상황 속에서 생성형 AI에 대해 규제를 강화해야 한다고 생각하는 국민이 늘어나고 있다.

[그림 2]는 2024년 4월 5일부터 4월 7일까지 18세 이상 3,129명을 대상으로 NHK에서 실시한 '생성형 AI의 규제'에 대한 여론 조사 결과인데, 응답자의 61%가 '규제를 강화해야 한다'라고 응답했으며 그 주된 이유로는 '가짜 정보로 인한 인권 침해가 우려되기 때문'을 꼽았다.

이렇듯 생성형 AI의 급속한 발달과 더불어 이에 대한 마땅한 규제 방법이 없는 현실 속에서 일본 문부과학성은 디지털 범죄 예방을 위해 관련 교육을 강조하고 있다는 상황이다.

2. 딥페이크 예방 교육

최근 인공지능(AI) 기술의 발전과 함께 딥페이크(deepfake) 영상이 사회적 문제로 떠오르면서 일본의 학교 현장에서도 '딥페이크 예방 교육'이 강화되고 있다. 딥페이크 기술은 특정 인물의 얼굴이나 음성을 조작하여 가짜 영상을 만들어내는 방식으로, 악용될 경우 명예훼손과 개인정보 침해 등 심각한 피해를 초래할 수 있다. 이에 일본 정부와 교육기관은 학생들에게 딥페이크의 위험성을 알리고, 예방 및 대응 방법을 교육하는 데 주력하고 있다.

특히 주목할만한 부분은 일본의 딥페이크 예방 교육은 단순히 딥페이크 범죄에 대한 경각심을 높이는 데 그치는 것이 아니라, 딥페이크 기술의 원리와 활용법을 함께 설명하는 방식으로 진행된다는 것이다. 구체적으로는 정보 과목을 통해 인공지능과 딥러닝의 개념을 제시함과 동시에 딥페이크 기술이 어떤 원리로 작동하는지 이해하도록 함으로써 학생들이 온라인상에서 접하는 영상이 조작되었을 가능성이 있음을 인지하고 비판적으로 정보를 분석하는 능력을 기를 수 있도록 교육이 진행된다.

[그림 3] 기시다 전 일본 총리 딥페이크 영상 (출처: NHK)

또한 딥페이크 기술이 범죄에 악용된 사례를 소개하고, 실제 피해 사례를 통해 그 심각성을 체감할 수 있도록 하는데, 이때 유명인의 얼굴을 합성한 허위조작정보나 학생들을 대상으로 한 불법 촬영물이 딥페이크 기술로 유포된 사례 등을 교육자료로 활용한다.

실제로 오사카에 사는 20대 남성은 단순히 재미로 기시다 전 일본 총리의 음성을 생성형 AI를 이용해 학습시켜 1시간 만에 딥페이크 영상을 만든 후 SNS에 공유했는데, 해당 영상이 2백만 회가 넘게 조회되고 뉴스에서도 다루어지는 등 사회적 문제가 된 바 있다. 따라서 학생들은 이러한 사례나 관련 자료들을 접하는 과정에서 딥페이크가 단순한 기술적 장난이 아니라 심각한 범죄 행위라는 사실을 깨닫게 된다.

법적 대응 방안에 대한 교육 또한 일본의 딥페이크 예방 교육에서 중요하게 다루어지는 부분인데, 일본의 형법과 개인정보보호법, 명예훼손에 관한 법률을 중심으로 딥페이크 제작 및 유포가 처벌 대상이 될 수 있음을 명확히 설명하고 있다. 이를 위해 학교에서는 경찰청과 협력해 정기적으로 관련 강연을 진행함으로써 학생들이 이러한 법적 지식을 접할 수 있는 기회를 제공하고 있다. 참고로 경찰청은 사이버 범죄 전문 경찰관이 학교에 방문할 수 있도록 함으로써 학생들에게 실제 수사 사례를 소개하고 법적 책임과 피해 예방 방법을 알리는 등 보다 효과적인 딥페이크 예방 교육이 이루어질 수 있도록 노력을 기울이고 있다.

이 외에도 일본에서는 시청각 자료를 활용해 딥페이크 예방 교육을 실시함으로써 학생들의 참여를 유도하고 있는데, 실제 딥페이크 영상과 원본 영상을 비교하여 기술적 차이를 직접 확인하도록 함으로써 가짜 영상을 판별하는 방법을 배우게 하는 것이다. 이러한 방법은 딥페이크 영상 등 학생들의 조작 콘텐츠 구별 능력 향상에 큰 도움이 된다.

[그림 4] 가짜 정보 관련 역할극 활동 (출처: NHK)

일본에서는 효과적인 딥페이크 예방 교육을 위해 토론 수업과 역할극을 활용하기도 하는데, 학생들은 가상의 상황을 설정하고 딥페이크 피해자가 되었을 때의 대처 방법을 고민하며 해결책을 모색한다. [그림 4]는 2016년 발생한 쿠마모토 지진 당시 동물원에서 동물들이 탈출했다며 SNS를 통해 일본 전국에 확산된 가짜 정보인데, 이러한 상황을 제시한 후 학생들이 가짜 정보를 공유한 사람이나 가짜 정보로 인해 곤란한 동물원 직원 등이 되어 역할극을 진행해 보도록 하는 것이다. 이러한 교육을 통해 학생들은 딥페이크 관련 피해 발생 시 신속하게 대응할 수 있는 능력을 갖추게 되며, 딥페이크 영상의 제작이나 유포가 타인에게 심각한 피해를 줄 수 있다는 점을 인식하게 된다.

이 외에도 일부 학교에서는 딥페이크 예방을 위한 프로젝트 학습을 도입하기도 했다. 학생들은 직접 인터넷에서 가짜 뉴스 사례를 분석하거나 AI 기술을 활용해 영상이 조작되었는지 판별하는 프로그램을 체험하면서 생성형 AI 기술에 대한 이해도를 높이는데, 이러한 교육은 학생들이 딥페이크의 위험성을 이론적으로 배우는 것을 넘어 실생활에 직접 적용하고 일상 속에서 피해를 예방하려는 노력을 기울이는데 도움이 된다.

3. 교육 활동 사례 및 관련 자료

가. 교육 활동 사례

 [미우라 시립 미나미시모우라 중학교]	- 중학교 2학년과 3학년 학생을 대상으로 원격으로 진행함. - 최근 발생한 러시아의 우크라이나 침공에 대한 딥페이크 영상을 소개함으로써 딥페이크로 인한 피해와 위험성을 제시하고, 전쟁이나 재해 발생 시 거짓 정보가 퍼지기 쉽다는 내용을 강조함.

 [기노완 시립 시신시 초등학교]	- 기노완 경찰서 소년과에서 학교를 방문하여 '안전하게 인터넷을 이용하는 방법'을 주제로 강연을 진행함. - 강연에 참여한 5학년 학생은 "스마트폰이 좋은 점도 있지만, 스마트폰으로 범죄를 저지르거나 SNS에 나쁜 말을 쓰는 사람도 있다는 것을 배웠다. 범죄에 연루되지 않도록 조심하겠다."고 소감을 밝힘.
 [히로시마 현립 후쿠야마 이요 고등학교]	- 히로시마현 경찰 사이버범죄대책과에서 학교를 방문해 10대가 피해를 당하기 쉬운 범죄 및 SNS를 통해 범죄에 가담하는 암거래 아르바이트 등의 실제 사례를 바탕으로 강연을 진행함. - 동시에 SNS 이용에 대한 동영상 시청을 통해 SNS의 위험성을 강조함.
 [요코하마 시립 구로스다 초등학교]	- 약 30명의 5학년 학생을 대상으로 딥페이크 영상 예방 교육을 진행함. - 이후 인터뷰 체험 게임을 통해 학생들이 번갈아 가며 기자의 역할을 맡아 인터뷰를 진행하고, 다른 학생의 면접을 진행하는 과정에서 거짓 정보를 식별하는 활동을 진행함.

나. 관련 자료

 [사이버 경찰 게임]	- 아이치현 경찰서에서 개발한 보드게임 형태의 교구. - 초등학생들이 일상생활에서 접할 수 있는 인터넷 범죄에 대처하는 방법을 배울 수 있도록 개발됨. - 게임판, 퀴즈 카드, 문제 발생 카드 등의 게임 키트가 제공되며, 게임 규칙을 설명하는 매뉴얼은 물론 학생용 워크시트 등이 제공되어 학급 상황에 따라 다양하게 활용 가능함.
 [최신 사이버범죄 퇴치 BOOK]	- 전국 방범 협회 연합회에서 개발한 교재 - 2021년 사이버 범죄로 검거 건수는 역대 최고인 12,209건으로, 사이버 공간 관련 범죄의 위협은 다양한 세대에 걸쳐 문제가 되고 있음. - 이러한 상황을 감안하여 인터넷을 안심하고 이용할 수 있도록 사이버 범죄로 인한 피해 방지 및 구체적 대책을 설명하는 책자를 개발함.

 [인터넷 안전 규칙]	- 전국 방범 협회 연합회에서 개발한 교재 - 최근 인터넷을 이용한 범죄와 괴롭힘은 증가하고 있으며, 특히 학교 현장에 1인 1단말기가 보급됨에 따라 해당 사례도 급증하고 있음. - 이에 아동이 피해자가 되지 않도록 보호하기 위한 대책이 담긴 책자를 개발함.

4. 맺음말

일본은 생성형 AI의 급격한 발달 상황 속에서 '표현의 자유'라는 측면과 AI로 인한 인권 침해 등의 '범죄 예방' 사이에서 균형을 잡기 위한 노력을 기울이고 있으며 이를 위해 초등학생부터 고등학생에 이르기까지 광범위한 관련 교육을 학교를 중심으로 진행하고 있다.

동시에 학교 교육과 더불어 가정 및 지역 사회의 역할도 강조하고 있는데 문부과학성은 학부모들을 대상으로 온라인 강의를 제공함으로써 자녀와 함께 딥페이크 관련 윤리 교육을 진행하도록 권장하고 있다. 또한 지역 사회와 협력하여 사이버 안전 캠페인을 전개하고, SNS나 인터넷 사용 시 주의해야 할 점을 지속적으로 홍보하고 있다.

한편 일본 정부는 딥페이크 범죄 예방을 위한 법적 장치를 강화하는 한편, 학교에서의 디지털 윤리 교육을 더욱 체계적으로 운영할 방침이다. 전문가들은 학생들이 어릴 때부터 올바른 정보 활용법을 익히고 디지털 기술의 부작용을 이해하는 것이 무엇보다 중요하다고 강조한다.

딥페이크 기술이 점점 정교해지고 있는 만큼, 이를 악용한 디지털 범죄도 다양화되고 더욱 증가할 가능성이 높다. 이에 일본 교육계는 학생들이 생성형 AI를 비롯한 디지털 기술을 올바르게 이해하고 피해를 예방할 수 있도록 지속적인 교육과 지원을 이어갈 계획이다.

【참고 자료】

- 高知県, https://www.pref.kochi.lg.jp/doc/2015070700147/
- 愛知県警察, https://www.pref.aichi.jp/police/anzen/cyber/game/cyberpolicegame.html
- 文部科学省, https://www.mext.go.jp/zyoukatsu/moral/
- 全国防犯協会連合会, https://www.bohan.or.jp/protect/net.html#:~:text=
- 日テレ, https://www.ntv.co.jp/jugyou/
- NHK, https://www3.nhk.or.jp/news/html/20231208/k10014275041000.html