

딥페이크 기술 대응 법제도 개선 방안 연구

(Research on measures to enhance legal system
in response to deepfake technology)

김경환/양진영 외

2020. 12

연구기관 : 법무법인 민후



이 보고서는 2020년도 방송통신위원회 방송통신발전기금 방송통신
융합 정책연구사업의 연구결과로서 보고서 내용은 연구자의 견해
이며, 방송통신위원회의 공식입장과 다를 수 있습니다.

제 출 문

방송통신위원회 위원장 귀하

본 보고서를 『딥페이크 기술 대응 법제도 개선 방안 연구』의 연구결과보고서로 제출합니다.

2020년 12월

연구기관 : 법무법인 민후

총괄책임자 : 김경환

참여연구원 : 양진영 최주선

허준범 김도윤

임한결 현수진

이지원

목 차

요 약 문	
제1장 서론	1
제1절 연구의 배경 및 필요성	1
제2절 연구의 목표 및 내용	3
제2장 딥페이크 기술 관련 기술 및 해외 입법 등 대응 동향 분석	4
제1절 딥페이크 관련 기술 동향	4
1. 딥페이크(deepfake)의 정의	4
2. 딥페이크 생성 기술의 발전	5
2.1. 딥페이크 생성 기술 개요	5
2.1.1. 오토인코더(Autoencoder) 기술	5
2.1.2. 적대적 생성 신경망(GAN) 기술	9
2.2. 딥페이크 생성 기술 동향	12
3. 딥페이크 감별 기술의 발전	17
3.1. 딥페이크 감별 기술의 등장 및 한계	17
3.2. 딥페이크 감별 기술 동향	18
3.3. 딥페이크 감별 기술을 위한 데이터베이스 구축	23
3.4. 블록체인을 이용한 딥페이크 감별	25
4. 딥페이크 기술에 대한 평가	27
4.1. 딥페이크 기술의 유용성	27
4.2. 딥페이크 기술의 문제점과 대책	28
5. 소결	29
제2절 딥페이크 관련 해외 입법 동향	31

1. 서설	31
2. 미국	31
2.1. 연방차원의 딥페이크 관련 입법 현황	31
2.1.1. 통신품위법과 온라인 성매매 퇴치법	31
2.1.2. 2018 악성 딥페이크 방지법	35
2.1.3. 2019년 딥페이크 보고법 (Deepfakes Report Act of 2019)	38
2.1.4. 2019년 책임법에 따라 부당한 이용으로부터 유래한 허위의 외관으로부터 모든 사람들을 보호하기 위한 법률	41
2.2. 각 주 별 딥페이크 관련 입법 현황	51
2.2.1. 뉴욕주	51
2.2.2.1. 프라이버시권 및 퍼블리시티권에 관한 민권법을 개정하고, 퍼블리시티권 침 해 조치 개시의 적시성에 관한 민사관행법 및 규칙을 개정하는 법안	52
2.2.2.2. 퍼블리시티권을 확립하고 성적으로 명백한 묘사를 불법적으로 유포하거나 출판하기 위하여 사적 권리를 제공하는 것과 관련한 민권법 개정법	55
2.2.2. 버니지아 주	59
2.2.3. 텍사스 주	61
2.2.4. 매사추세츠 주	62
2.2.5. 캘리포니아 주	64
2.2.6. 메릴랜드 주	67
2.2.7. 미시간 주	69
2.3. 소결	71
3. EU 및 유럽국가	71
3.1. EU	71
3.2. 프랑스	74
3.3. 독일	80
4. 호주	82

5. 중국	87
6. 일본	93
7. 결어	95

제3장 딥페이크 기술 관련 국내 입법 현황 및 개선논의 79

제1절 서설	97
제2절 딥페이크 관련 법적이슈와 국내 입법 현황	99
1. 음란물	99
가. 서설	99
나. 성폭력범죄의 처벌 등에 관한 특례법	99
다. 정보통신망 이용촉진 및 정보보호 등에 관한 법률	103
라. 소결	104
2. 명예훼손·사자명예훼손	104
가. 서설	104
나. 형법	105
다. 정보통신망 이용촉진 및 정보보호 등에 관한 법률	106
라. 소결	106
3. 퍼블리시티권·초상권 침해	107
가. 퍼블리시티권	107
나. 초상권	107
다. 소결	108
4. 저작권	109
5. 보이스피싱	111
가. 서설	111
나. 전기통신금융사기 피해 방지 및 피해금 환급에 관한 특별법	111
다. 소결	113
6. 선거	113

가. 서설	113
나. 공직선거법	113
다. 소결	116
7. 피해자의 삭제, 처리정지 등 조치요구	117
가. 서설	117
나. 개인정보보호법	117
다. 정보통신망 이용촉진 및 정보보호 등에 관한 법률	121
라. 성폭력범죄의 처벌 등에 관한 특례법 일부개정법률안	123
마. 소결	125
8. 플랫폼 운영자의 책임과 의무	125
가. 서설	125
나. 정보통신망 이용촉진 및 정보보호 등에 관한 법률	126
1) 플랫폼 운영자의 불법정보 유통금지 의무	126
2) 불법정보 삭제·임시조치 등	128
3) 불법촬영물등 유통방지 책임자 지정	130
4) 투명성 보고서 작성 및 제출	133
다. 전기통신사업법	134
라. 소결	136
9. 정부의 시책마련	138
가. 서설	139
나. 정보통신망 이용촉진 및 정보보호 등에 관한 법률	139
다. 소결	141
10. 결어	141
제3절 딥페이크 관련 법적이슈와 국내 입법개선 논의	145
1. 성폭력범죄의 처벌 등에 관한 특례법	145
가. 서설	145

나. 성폭력처벌법 제14조의2 제1항 목적조항 삭제여부	145
다. 딥페이크 음란물 소지 행위에 대한 처벌규정 신설여부	149
라. 소결	151
2. 정보통신망 이용촉진 및 정보보호 등에 관한 법률	152
3. 공직선거법	153
가. 서설	153
나. 해외 입법례 검토	154
다. 소결	157
4. 결어	157

제4장 딥페이크 기술 관련 국내 제도 현황 및 개선논의 9

제1절 서설	159
제2절 딥페이크 관련 사전규제 방안	161
1. 딥페이크 유통신고·허가제	161
가. 서설	161
나. 딥페이크 유통신고·허가제의 도입가능성	161
다. 소결	165
2. 결어	165
제3절 딥페이크 관련 사후규제 방안	167
1. 워터마크·전자서명 등을 이용한 딥페이크 표시의무제도	167
1.1. 서설	167
1.2. 디지털 워터마크	167
가. 개념	167
나. 디지털 워터마크의 기술 개요	168
다. 디지털 워터마크 관련 국내외 제도 및 입법현황	171
1) 국내의 경우	171
2) 해외의 경우	173

3) 소결	175
라. 적용 및 한계점	175
1.3. 전자서명	176
가. 개념	176
나. 전자서명 관련 국내외 제도 및 입법현황	177
1) 국내의 경우	177
2) 해외의 경우	179
다. 적용 및 한계점	181
1.4. 라벨	181
가. 개념	181
나. 라벨 관련 제도 및 입법현황	181
다. 적용 및 한계점	182
1.5. 워터마크 표시의무제도의 도입	183
가. 워터마크 표시의무제도의 적용 범위의 문제	183
나. 관계 법령 상 워터마크 표시의무제도 도입검토	185
1) 성폭력처벌법 상 허위영상물 등에 대한 워터마크 표시의무	185
2) 정보통신망법 상 불법정보에 대한 워터마크 표시의무	186
3) 공직선거법 상 허위영상에 대한 워터마크 표시의무	191
1.6. 결어	192
2. 딥페이크 변경내용 표시의무제도	193
가. 개념	193
나. 변경내용 표시의무 관련 국내외 제도 및 입법현황	193
1) 국내의 경우	193
2) 해외의 경우	193
다. 관계 법령 상 변경내용 표시의무제도 도입검토	194
1) 정보통신망법 상 불법정보에 대한 변경내용 표시의무	195

2) 공직선거법 상 허위영상에 대한 변경내용 표시의무	196
라. 결어	198
3. 기타 딥페이크에 대한 사후규제 방안	199
4. 결어	200
제4절 딥페이크 피해자의 구제강화 방안	201
1. 피해자의 삭제요구권 강화	201
2. 국내대리인 지정 제도의 활용	204
가. 국내대리인 지정 제도의 개념	204
나. 적용 및 한계점	205
3. 결어	207
제5절 딥페이크 식별 기술의 지원	208
1. 서설	208
2. 딥페이크 식별 및 인증을 위한 기관 지정 또는 설립 근거규정 마련	208
가. 기존의 논의	208
나. 정보통신망법 상 딥페이크 식별 및 인증을 위한 기관 근거규정 마련	212
1) 서설	212
2) 정보통신망법 상 인증기관 지정 근거규정 마련	213
3) 정보통신망법 상 기관 설립 근거규정 마련	216
3. 딥페이크 식별 기술 및 재정 지원을 위한 근거규정 마련	217
가. 딥페이크 식별 기술 지원 현황	217
1) 국내의 경우	217
가) 서울대학교·한국정보화진흥원의 딥페이크 탐지 AI 경진대회 개최	217
나) 과학기술정보통신부의 AI 학습용 데이터 구축 사업 확정	218
2) 해외의 경우	220
3) 소결	220
나. 딥페이크 식별 기술 지원 방안	221

다. 딥페이크 식별 기술 지원 근거규정 마련	222
4. 결어	227
제6절 딥페이크 관련 범부처협의체 등의 운영	229
1. 서설	229
2. 딥페이크 관련 전담부서의 운영	230
가. 딥페이크 관련 전담부서의 업무	230
나. 음란물 및 선거물 관련	232
1) 음란물 관련	232
2) 선거 관련	233
3. 딥페이크 관련 범부처협의체 운영	234
4. 결어	235
제5장 결론	237
참 고 문 헌	243

표 목 차

<표 2-1> 주요 딥페이크 오픈 소스	12
<표 2-2> 딥페이크 감별 기술	22
<표 3-1> 성폭력처벌법 제14조 및 제14조의2 조문구성 비교	102
<표 3-2> 성폭력처벌법 일부개정법률안 신구조문 대비표	124
<표 3-3> 딥페이크 관련 이슈와 국내 관련 법령	141
<표 3-4> 딥페이크 기술로 제작된 음란영상물에 대한 해외 입법례	148
<표 3-5> 딥페이크 기술로 제작된 영상과 선거에 관한 해외 입법례	155
<표 4-1> 전자서명 관련 각국의 입법례	180
<표 4-2> 방송통신발전 기본법 제26조 개정안	211
<표 4-3> 정보통신망법 제4조 제2항 시책 관련 규정 중 기관 지정 관련 규정 ..	213
<표 4-4> 정보통신망법 상 기관에 대한 기술 및 재정 지원 관련 규정	225
<표 6-1> 딥페이크 기술 관련 입법 및 제도 개선 논의	239

그 립 목 차

[그림 2-1] Autoencoder의 구조	7
[그림 2-2] 오토인코더(Autoencoder) 방식을 사용한 딥페이크 영상 제작	9
[그림 2-3] 적대적 생성 신경망의 구조	10
[그림 2-4] GAN 기술에 대한 연구 수 증가 (arXiv 게재 수 기준)	11
[그림 2-5] 딥페이크 기술을 이용한 합성 예	13
[그림 2-6] 실시간 딥페이크 합성	13
[그림 2-7] 말라리아 퇴치 홍보 캠페인 영상 제작 과정	14
[그림 2-8] 삼성전자 AI연구센터가 만든 모나리자 동영상	15
[그림 2-9] 딥페이크 기술 활용 예	16
[그림 2-10] 적대적 생성 신경망으로 생성된 영상들의 품질변화	17
[그림 2-11] 실제 영상(좌)과 조작된 영상(우)의 비교	18
[그림 2-12] 투 스트림 신경망을 이용한 딥페이크 검출 알고리즘	19
[그림 2-13] CNN과 RNN을 사용하여 딥페이크 동영상을 검출하는 알고리즘을 도식화한 예	20
[그림 2-14] 캡슐 신경망 이용하여 조작된 동영상을 검출하는 방법의 개요	21
[그림 2-15] 블록체인 원리	25
[그림 2-16] 조작된 영상(좌)과 식별 기술을 통해 탐지한 결과(우)	27
[그림 4-1] 워터마킹 기술의 적용 과정	169
[그림 4-2] 뉴욕대 연구진이 개발한 새로운 형태의 사진 조작 검증방법	171
[그림 4-3] 전자서명의 생성과 검증 과정	177
[그림 4-4] 전자서명의 활용	178
[그림 5-1] 과학기술정보통신부 2020년 AI 학습용 데이터 구축 과제 선정 결과	219

요 약 문

1. 제 목

딥페이크 기술 대응 법제도 개선 방안 연구

2. 연구 목적 및 필요성

딥페이크(deepfake)는 딥러닝(Deep learning)과 페이크(fake)의 합성어로, 인공지능 기반 기술로 만들어진 진짜처럼 보이는 가짜 동영상, 음성파일 등을 말한다. 이러한 딥페이크 기술은 영상의 혁신으로 평가받으며 현재 상업영화, 의료용영상 등에서 활용되고 있다. 그러나 동시에 유명인을 대상으로 한 음란물 제작 또는 가짜뉴스 등 불법유해정보에 악용됨으로써 사회적인 논란을 일으키고 있다.

딥페이크 기술이 인류에게 주는 이로운 점이 분명히 있기에 무작정 딥페이크 기술의 발전을 막고 규제할 수는 없다. 딥페이크 기술이 비약적으로 발전하고 있는 상황에서 딥페이크 기술로 인한 사회적 부작용을 줄이고 순기능을 더욱 촉진할 수 있는 방향을 찾는 것이 바람직하다. 이를 위하여는 딥페이크 기술을 다루는 입법과 제도가 충분하게 뒷받침되어야 한다.

우리나라의 경우 딥페이크 기술이 등장한지 수년이 지났음에도 불구하고, 본격적인 딥페이크 관련 입법논의가 진행된지는 얼마되지 않았으며, 2020년 성폭력처벌법 제14조의 2가 신설된 것을 시초로, 최근에는 정보통신망법의 일부 법조항이 개정되었다. 다행히 이전에 비하여는 딥페이크 관련 입법논의가 꽤 진행되고 있으나, 법률신설안 및 개정안에 대한 추가적인 논의가 계속 필요하다.

현재 진행되고 있는 입법논의 및 정책을 구체화하고, 딥페이크 대응과 규제에 더욱 효과적으로 적용할 수 있는 신설안 또는 개정안을 마련하기 위하여는, 딥페이크 관련 기술 및 해외 입법 현황 조사가 선행되어야 한다. 또한 딥페이크 관련 법적 이슈 및 기존에 마련되어 있는 국내 규제체계를 파악하여 규제공백을 메우고 규제 사각지대를 해소할

필요성이 있다.

3. 연구의 구성 및 범위

본 연구의 목적은 딥페이크 기술과 관련된 기술동향 및 해외 입법, 정책 동향을 파악함으로써 이를 국내 입법 및 정책에 반영하고, 딥페이크 기술의 발전으로 인한 사회적 역기능 저하, 딥페이크로 인한 형사처벌 및 피해자의 구제를 종합적으로 고려하여 균형 있는 입법개선 방향 및 정책안을 제시하는 것이며, 구체적인 연구의 내용은 다음과 같다.

- 딥페이크 기술 관련 기술 개발 동향 및 해외 입법 등 대응 동향 분석
 - 해외 및 국내의 최신 딥페이크 기술 동향 조사·분석
 - 해외 주요국의 딥페이크 기술 관련 입법 및 정책 대응 조사·분석
- 딥페이크 기술 관련 입법 개선방안 제시
 - 국내 딥페이크 기술 관련 입법 현황 조사·분석
 - 국내 딥페이크 기술 관련 법령 제·개정 방향 제시
- 딥페이크 기술 관련 제도 개선방안 제시
 - 국내 딥페이크 기술 관련 제도 현황 조사·분석
 - 국내 딥페이크 기술 관련 제도 개선 및 근거규정 마련 방안 제시
- 딥페이크 기술 관련 규제체계 전반 등을 논의하기 위한 범부처 협의체 구성 제시
 - 딥페이크 관련 범부처협의체의 업무와 운영

4. 연구 내용 및 결과

딥페이크 생성기술은 문화컨텐츠, 의료 등 분야에서 유용한 기술로서 사용되고 있지만, 음란물 등 디지털성범죄, 명예훼손, 선거범죄 등에 악용될 가능성이 크다. 딥페이크 생성기술은 이윤창출의 효과가 분명하기에 급속도로 발전 중이다. 그러나 딥페이크 식별 기술의 발전은 더딘 상황이다. 딥페이크 기술로 인한 부작용을 줄이고, 피해를 예방하기 위하여 국가적인 차원에서 딥페이크 식별 기술 발전을 지원해야 할 필

요성이 있다.

해외에서는 이러한 딥페이크 기술에 대한 사회적 부작용을 줄이기 위하여 선제적으로 법률안을 마련하였으며, 그 중 몇몇 국가에서는 이미 관련 법이 시행 중이다. 딥페이크에 관하여 가장 적극적으로 입법활동을 하고 있는 국가는 미국이며, 미국 연방차원에서 입법 추진되고 있는 법안이 상당히 구체적이나 아직 본격적으로 시행되지는 않고 있다. 미국은 연방차원의 법안 이외의 각 주에서도 딥페이크를 음란물, 프라이버시, 명예훼손, 개인정보, 플랫폼 사업자의 책임, 선거, 가짜뉴스 등 여러 주제에서 접근하여 법을 마련하거나 입법이 추진되고 있다. 그 이외의 국가들은 딥페이크에 대하여 정면으로 다룬 독립된 법안을 가지고 있지 아니하나, 온라인콘텐츠, 플랫폼사업자, 선거, 부정확한 정보의 유통 방지 등 특정 이슈에 맞게 입법이 추진되거나 관련 법이 시행되고 있다.

딥페이크 기술은 음란물, 명예훼손, 퍼블리시티권, 초상권 침해, 저작권, 보이스포싱, 피해자의 삭제, 처리정지 등 조치요구, 정보통신서비스 제공자의 의무와 책임, 선거 등 법적이슈와 관련되어 있는데, 현재 국내에서는 딥페이크 관련하여 단독으로 법률안이 발의된 것은 없으며, 최근 딥페이크 기술로 제작한 음란영상물을 규제하기 위한 성폭력처벌법 제14조의2가 신설된 것을 시작으로, 정보통신망법에 딥페이크와 관련된 여러 조항이 도입되어 시행되고 있다. 정보통신망법에서는 과학기술정보통신부장관 또는 방송통신위원회로 하여금 딥페이크 관련 기술에 관한 정책을 마련하도록 하였고(정보통신망법 제4조 제2항 7의2호), 일정규모 이상의 정보통신서비스 제공자로 하여금 딥페이크 기술로 생성된 음란물의 유통을 방지하기 위한 책임자를 지정하고(동법 제44조의 9), 불법촬영물 등의 유통방지와 관련된 각종 사항에 대한 보고서 작성 및 제출 의무를 부여하였다(동법 제64조의5).

딥페이크 관련 이슈는 기존 국내 법령으로도 상당부분 해결되고 있는 상황이어서 심각한 입법공백이 있지는 아니한 것으로 보인다. 다만 성폭력처벌법 제14조의2(허위영상물 등의 반포등) 제1항 상 목적조항의 삭제 또는 유지여부, 성폭력처벌법 제14조의2 내 소지행위 처벌규정 신설여부가 검토되어야 할 것으로 보이며, 해외에서 딥페이크 관련 논의가 선거법 쪽에서 활발하게 일어나고 있는 것에 비하여 국내에서는 아직까지 이렇

다 할 개정작업이 진행되지 않고 있어, 해외 사례에 비추어 국내 공직선거법을 개선하여야 할지에 대한 추가적인 검토가 필요해 보인다.

이처럼 딥페이크 기술과 관련한 입법이 최근에서야 본격적으로 진행되고 있는 상황이며, 정보통신망법 상 딥페이크 식별 기술 개발, 보급 관련 시책마련 의무가 도입되어 있기는 하나, 아직 이렇다 할 구체적인 시책이 마련되지 않았고, 딥페이크 관련된 제도도 신설되지 않고 있다. 이에 앞으로 딥페이크 기술과 관련되어 어떤 제도를 시행하면 딥페이크로 인한 사회적인 부작용을 효과적으로 줄일 수 있을지, 그러한 제도의 도입을 위하여 입법적으로 어떻게 근거규정을 마련할지에 관하여 검토가 진행되었다.

딥페이크에 대한 사전규제책으로서의 유통 신고·허가제가 있을 수 있으나, 헌법상 사전검열에 해당하여 실제로 추진하기 쉽지 않다. 딥페이크에 관한 사후규제책으로 딥페이크 영상 생성 이후 유통시 워터마크 표시의무, 변경내용표시의무 제도를 도입하는 것을 검토해볼 수 있으며, 정보통신망법 상 근거규정을 마련하여 시행하면 될 것으로 보인다. 그 외 사후규제책으로서, 플랫폼 보류대기 시스템, 지정플랫폼의 운영 등을 검토해볼 수 있으나, 아직 딥페이크 식별 기술이 완전하지 못하고 대중적으로 보급되지 않은 점, 자칫하면 사전허가제로 변질되어 운영될 우려가 있다는 점 등 때문에 실제 시행은 쉽지 않아 보인다.

한편, 딥페이크 피해자의 구제강화 방안으로 딥페이크 피해자의 삭제요구권 강화, 국내대리인 지정제도의 활용을 고려해볼 수 있으며, 딥페이크 식별 기술의 발전을 위해 딥페이크 식별 및 인증을 위한 기관 지정 또는 설립, 정부 차원에서의 딥페이크 식별 기술에 대한 지원이 고려될 수 있다.

마지막으로 딥페이크 활용/악용 실태 파악, 모니터링, 워터마크 표시의무제도 등 관련 제도관리, 유통규제, 식별 기술, 보급을 위한 시책마련, 관련 법안 발의 및 법률제개정, 기술 배포 및 상용화 지원, 보고서 작성 등 딥페이크 관련 여러 업무를 총괄적으로 처리하기 위한 전담부서의 지정을 고려해볼 수 있다.

나아가 딥페이크 기술에 관한 각 부서 간 추진업무의 통일성을 기하고, 부처 간 협업을 통해 효율적인 정책을 연구 및 추진하기 위하여 방송통신위원회, 과학기술정보통신

부, 법무부, 경찰청 등으로 구성된 딥페이크 기술 관련 범부처협의체의 구성이 요구되는 바이다.

5. 정책적 활용 내용

본 연구는 지금까지 본격적으로 검토되지 아니한 국내 딥페이크 관련 법적이슈를 총망라하여 분석하고, 현행 법령의 입법공백을 찾아 입법 개선안을 제시하는 것으로서 실제 입법활동에 자료로 활용될 수 있다.

현재 국내에서 딥페이크 관련한 제도와 정책이 시행되고 있지 아니하며 도입검토 단계에 불과하나, 본 연구에서는 실질적으로 국내에 도입가능한 딥페이크 제도를 검토하고 도입시 필요한 근거법령, 관련 기관, 부처 등을 제시하였는바, 향후 제도 기획 단계에서 자료로 활용될 수 있다.

6. 기대효과

본 연구는 딥페이크 관련 입법의 가이드라인을 제시하였는바 규제공백이 없는 입법이 이루어질 것으로 기대한다. 또한 본 연구에서는 해외 딥페이크 관련 법령을 구체적으로 검토하였는바, 향후 국내 입법 및 제도 개선에 기여할 것으로 기대한다. 마지막으로 본 연구는 딥페이크 식별 기술의 발전 및 법령 상 피해구제 방안의 강화에 관한 의견을 제시하였는바, 본 연구에서 제안한 방향으로 입법 및 제도가 개선되는 경우 딥페이크로 인한 사회적인 부작용이 최소화되고, 피해자가 신속하고 효과적으로 구제받을 수 있을 것으로 기대한다.

SUMMARY

1. Title

Research on measures to enhance legal system in response to deepfake technology

2. Objective and Importance of Research

It is obvious that deepfake technology benefits mankind and thus, development of the technology cannot be blindly forbidden and regulated. In a situation where deepfake technology is developing rapidly, it is desirable to find a direction to reduce social side-effects caused by deepfake technology and further promote positive functions. To this end, legislation and systems to handle deepfake technology should be fully supported. In order to materialize ongoing legislative discussion and policies and establish new or amended bills, which are able to apply to responding to and regulating deepfake, research on technology and current status of overseas legislation in relation to deepfake should be preceded. Moreover, it is necessary to address regulatory gap and remove blind spot of regulations by identifying legal issues concerning deepfake and domestic regulation systems established previously.

3. Contents and Scope of the Research

· Analysis of the trend of technology development and tendency of responding including legislation, with regard to deepfake technology

- Research on analysis of trend of latest deepfake technology in foreign countries and Korea
- Research on analysis of legislation and policies in response to deepfake

technology in major foreign countries

- Suggestions for enhancement of legislation regarding deepfake technology
 - Research on analysis of current status of legislation concerning deepfake technology in Korea
 - Presentation of directions of enactment · amendment of laws regarding deepfake technology in Korea
- Suggestions for improvement of systems related to deepfake technology
 - Research on Analysis of current status of systems related to deepfake technology in Korea
 - Suggestions for improvement of systems and establishment of evidential regulations regarding deepfake technology in Korea
- Presentation of forming pan-departmental consultative committee to discuss overall regulation systems regarding deepfake technology, etc.
 - Tasks and operation of pan-departmental consultative committee concerning deepfake

4. Research Results

As many of the issues with regard to deepfake are being resolved under existing domestic laws, it seems that there is no critical legislative gap. However, it is deemed that deletion or maintenance of the purpose provision under Paragraph 1 of Article 14-2 (Distribution, etc. of Fake Pictures, etc.) of Act on Special Cases Concerning the Punishment, etc., of Sexual Crimes and new establishment of provision of act of possession in Article 14-2 thereof are necessary to be reviewed. In addition, while the issue of deepfake is being discussed actively in the part of the election act in foreign countries, noticeable revision has not yet proceeded in Korea, and thus additional review seems to be required for the matter if Public Official Election Act in Korea is

needed to be improved in light of overseas examples.

There may be a distribution report·permission system, as a pre-regulatory measure for deepfake but it is not easy to be proceeded since it falls under pre-censorship under Constitution. As ex-post regulatory measures for deepfake, adopting systems which oblige people to display watermark and items changed at the time of distribution after generating deepfake video can be considered, and it seems that it can be implemented by establishing evidential regulations under Act on Promotion of Information and Communications Network Utilization and Data Protection, etc. Operation of platform waiting systems and designated platforms, etc. can be considered as other ex-post measures but it is not likely that those can be easily implemented due to the fact that deepfake detection technology has not yet been completed and has not become commonly available to all, there are concerns that it could be changed into a system requiring prior permission to operate, etc.

Meanwhile, as a measure to strengthen remedies for deepfake victims, enhancement of the victim's right to request deletion and utilization of the system to designate a proxy in Korea can be considered. Moreover, in order to develop deepfake detection technology, designation or establishment of institutions for deepfake detection and verification and support for deepfake detection technology at the government level can be considered.

Lastly, designation of a responsible department for the purpose of handling various tasks regarding deepfake comprehensively such as grasping the state of utilization/abuse of deepfake, monitoring, management of systems including a system to oblige people to display watermark, regulation of distribution, coming up with policies to popularize detection technology, proposing relevant bills and enactment·revision of laws, distribution of technology and support for being ready for the public, preparing reports, etc. can be considered.

Furthermore, it is required to form a pan-departmental consultative committee for deepfake technology consisting of Korea Communications Committee, Ministry of Science and ICT, Ministry of Justice, National Policy Agency, etc. to ensure unity of tasks proceeded by each department in relation to deepfake technology and to study and push ahead with effective policies through coordination between departments.

5. Policy Suggestions for Practical Use

This research can be utilized as materials for actual legislation by fully covering and analyzing legal issues concerning deepfake in Korea which have not yet been reviewed in earnest, and finding legislative gaps in current laws and suggesting legislative improvements.

Currently, systems and policies regarding deepfake are not implemented in Korea and are in the stage of review for introduction. In this study, however, as evidential laws, relevant institutions, ministries, etc. necessary for reviewing and introducing deepfake systems available to introduce in Korea are presented, it can be utilized as materials in the stage of planning of systems further.

6. Expectations

This research has provided guidelines for legislation regarding deepfake and it is expected to be legislated without a regulatory gap. In addition, in this study, deepfake-related statute in foreign countries are reviewed in detail, and thus, it is forecast to contribute to enhancement of domestic legislation and systems. Finally, as opinions on development of deepfake detection technology and strengthening of remedies under statute are presented in this research, if legislation and systems are improved in the direction suggested in this study, social side effects will be minimized and victims will receive remedies promptly and effectively.

CONTENTS

Chapter 1. Introduction

Research on measures to enhance legal system in response to deepfake technology

Chapter 2. Objective and Importance of Research

Deepfake, a combination of the words Deep learning and Fake, which is made with artificial intelligence-based technology, refers to fake videos and voice files that look real. Such deepfake technology gains a reputation as a revolution of videos and is being utilized in commercial movies, medical videos, etc. At the same time, however, it causes social controversy by being abused for illegal and harmful information including producing pornography using celebrities and false news.

It is obvious that deepfake technology benefits mankind and thus, development of the technology cannot be blindly forbidden and regulated. In a situation where deepfake technology is developing rapidly, it is desirable to find a direction to reduce social side-effects caused by deepfake technology and further promote positive functions. To this end, legislation and systems to handle deepfake technology should be fully supported.

In Korea, even though it has been several years since deepfake technology has emerged, legislation regarding deepfake has not been discussed for very long, and starting with establishment of Article 14-2 of Act on Special Cases Concerning the Punishment, etc. of Sexual Crimes in 2020, some of provisions in Act on Promotion of Information and Communications Network Utilization and Information Protection, etc. have been amended recently. Fortunately, legislative discussion on deepfake are quite

ongoing compared to the past but further discussions for new legislative bills and amendments are still necessary.

In order to materialize ongoing legislative discussion and policies and establish new or amended bills, which are able to apply to responding to and regulating deepfake, research on technology and current status of overseas legislation in relation to deepfake should be preceded. Moreover, it is necessary to address regulatory gap and remove blind spot of regulations by identifying legal issues concerning deepfake and domestic regulation systems established previously.

Chapter 3. Contents and Scope of the Research

This study aims to identify technology trends and overseas legislation and policy trends in relation to deepfake and reflect them in domestic legislation and policies and present balanced directions for enhancement of legislation and policies by comprehensively considering a decrease in social adverse effects caused by development of deepfake and criminal punishment for deepfake and remedies for victims. Details of the study are described as follows:

- Analysis of the trend of technology development and tendency of responding including legislation, with regard to deepfake technology
 - Research on analysis of trend of latest deepfake technology in foreign countries and Korea
 - Research on analysis of legislation and policies in response to deepfake technology in major foreign countries
- Suggestions for enhancement of legislation regarding deepfake technology
 - Research on analysis of current status of legislation concerning deepfake technology in Korea
 - Presentation of directions of enactment · amendment of laws regarding deepfake

technology in Korea

- Suggestions for improvement of systems related to deepfake technology
 - Research on Analysis of current status of systems related to deepfake technology in Korea
 - Suggestions for improvement of systems and establishment of evidential regulations regarding deepfake technology in Korea
- Presentation of forming pan-departmental consultative committee to discuss overall regulation systems regarding deepfake technology, etc.
 - Tasks and operation of pan-departmental consultative committee concerning deepfake

Chapter 4. Research Results

Technology to generate deepfake is utilized as a useful technology in the area of cultural content, medical care, etc. but there are possibilities to be abused for digital sex crimes including pornography, defamation, election offenses, etc. Such technology is rapidly developing on the back of its effects to create profits. However, development of detection technology is slow in progress. In order to reduce side effects caused by deepfake technology and to prevent damages, deepfake detection technology is required to be supported at the national level.

For the purpose of reducing social side effects on deepfake technology, foreign countries have prepared bills preemptively and relevant laws have already come into effect in some of those countries. The country that the most actively legislating concerning deepfake is the United States and bills, which are being legislated at the U.S. federal level, are quite specific, but it has not yet been enforced in earnest. In addition to the bills at the federal level, each state of the U.S. is drafting laws or proceeding legislations by approaching to deepfake on the basis of various topics

including pornography, privacy, defamation, personal information, responsibility of platform providers, election, false news, etc. Other countries do not have independent bills which deal with deepfake directly but legislation is being proceeded or relevant laws are in effect with regard to specific issues such as online content, platform business, election, prevention of distribution of incorrect information.

Deepfake technology is related to legal issues such as pornography, defamation, publicity rights, violation of portrait rights, copyrights, voice phishing, deletion of victims, demands of actions including suspension of processing, obligations and responsibility of information and communication service provider, election and currently, in Korea, no bill has been proposed solely for deepfake but starting with recent establishment of Article 14-2 of Act on Special Cases Concerning the Punishment, etc. of Sexual Crimes to regulate pornographic videos produced by deepfake technology, several provisions regarding deepfake are introduced in Act on Promotion of Information and Communications Network Utilization and Information Protection, etc. and are in effect. In accordance with Act on Promotion of Information and Communications Network Utilization and Information Protection, etc., the Minister of Science and ICT or the Korea Communications Commission shall formulate policies for deepfake-related technology (Subparagraph 7-2 of Paragraph 2 of Article 4), an information and communications service provider over a certain scale shall designate a responsible person to prevent distribution of pornography produced with deepfake technology (Article 44-9), and is responsible for preparing and submitting reports on various matters regarding prevention of distribution of illegal photos and videos, etc.(Article 64-5)

As many of the issues with regard to deepfake are being resolved under existing domestic laws, it seems that there is no critical legislative gap. However, it is deemed that deletion or maintenance of the purpose provision under Paragraph 1 of Article

14-2 (Distribution, etc. of Fake Pictures, etc.) of Act on Special Cases Concerning the Punishment, etc., of Sexual Crimes and new establishment of provision of act of possession in Article 14-2 thereof are necessary to be reviewed. In addition, while the issue of deepfake is being discussed actively in the part of the election act in foreign countries, noticeable amendment has not yet proceeded in Korea, and thus, additional review seems to be required for the matter if Public Official Election Act in Korea is needed to be improved in light of overseas examples.

As mentioned as above, legislation concerning deepfake technology has been progressing just recently, and although obligations to develop deepfake detection technology and to formulate policies to distribute are introduced under Act on Promotion of Information and Communications Network Utilization and Information Protection, etc., specific policies have not yet prepared and systems regarding deepfake have not yet established as well. Therefore, for further deepfake technology, what systems would effectively reduce social side effects caused by deepfake, and how to prepare evidential regulations in terms of legislation in order to introduce such systems are reviewed.

There may be a distribution report·permission system, as a pre-regulatory measure for deepfake but it is not easy to be proceeded since it falls under pre-censorship under Constitution. As ex-post regulatory measures for deepfake, adopting systems which oblige people to display watermark and items changed at the time of distribution after generating deepfake video can be considered, and it seems that it can be implemented by establishing evidential regulations under Act on Promotion of Information and Communications Network Utilization and Data Protection, etc. Operation of platform warning systems and designated platforms, etc. can be considered as other ex-post measures but it is not likely that those can be easily implemented due to the fact that deepfake detection technology has not yet been completed and has not

become commonly available to all, there are concerns that it could be changed into a system requiring prior permission to operate, etc.

Meanwhile, as a measure to strengthen remedies for deepfake victims, enhancement of the victim's right to request deletion and utilization of the system to designate a proxy in Korea can be considered. Moreover, in order to develop deepfake detection technology, designation or establishment of institutions for deepfake detection and verification and support for deepfake detection technology at the government level can be considered.

Lastly, designation of a responsible department for the purpose of handling various tasks regarding deepfake comprehensively such as grasping the state of utilization/abuse of deepfake, monitoring, management of systems including a system to oblige people to display watermark, regulation of distribution, coming up with policies to popularize detection technology, proposing relevant bills and enactment·revision of laws, distribution of technology and support for being ready for the public, preparing reports, etc. can be considered.

Furthermore, it is required to form a pan-departmental consultative committee for deepfake technology consisting of Korea Communications Committee, Ministry of Science and ICT, Ministry of Justice, National Policy Agency, etc. to ensure unity of tasks proceeded by each department in relation to deepfake technology and to study and push ahead with effective policies through coordination between departments.

Chapter 5. Policy Suggestions for Practical Use

This research can be utilized as materials for actual legislation by fully covering and analyzing legal issues concerning deepfake in Korea which have not yet been reviewed in earnest, and finding legislative gaps in current laws and suggesting legislative improvements.

Currently, systems and policies regarding deepfake are not implemented in Korea and are in the stage of review for introduction. In this study, however, as evidential laws, relevant institutions, ministries, etc. necessary for reviewing and introducing deepfake systems available to introduce in Korea are presented, it can be utilized as materials in the stage of planning of systems further.

Chapter 6. Expectations

This research has provided guidelines for legislation regarding deepfake and it is expected to be legislated without a regulatory gap. In addition, in this study, deepfake-related statute in foreign countries are reviewed in detail, and thus, it is forecast to contribute to enhancement of domestic legislation and systems. Finally, as opinions on development of deepfake detection technology and strengthening of remedies under statute are presented in this research, if legislation and systems are improved in the direction suggested in this study, social side effects will be minimized and victims will receive remedies promptly and effectively.

제1장 서론

제1절 연구의 배경 및 필요성

딥페이크(deepfake)는 딥러닝(Deep learning)과 페이크(fake)의 합성어로, 인공지능 기반 기술로 만들어진 진짜처럼 보이는 가짜 동영상, 음성파일 등을 말한다. 더욱 구체적으로 딥페이크 기술이란 사람을 대상으로 한 영상에 인공지능 기술을 이용하여 타인의 얼굴이나 신체 부위의 이미지를 중첩하거나 결합함으로써 일반인이 합성 여부를 확인하는 것이 사실상 불가능한 가공의 영상을 만드는 기술이다.

이러한 딥페이크 기술은 영상의 혁신으로 평가받으며 현재 상업영화, 의료용영상 등에서 활용되고 있다. 그러나 동시에 유명인을 대상으로 한 음란물 제작 또는 가짜 뉴스 등 불법유해정보에 악용됨으로써 사회적인 논란을 일으키고 있다.

딥페이크 기술이 인류에게 주는 이로운 점이 분명히 있기에 무작정 딥페이크 기술의 발전을 막고 규제할 수는 없다. 딥페이크 기술이 비약적으로 발전하고 있는 상황에서 딥페이크 기술로 인한 사회적 부작용을 줄이고 순기능을 더욱 촉진할 수 있는 방향을 찾는 것이 바람직하다. 이를 위하여는 딥페이크 기술을 다루는 입법과 제도가 충분하게 뒷받침되어야 한다.

우리나라의 경우 딥페이크 기술이 등장한지 수년이 지났음에도 불구하고, 본격적인 딥페이크 관련 입법논의가 진행된지는 얼마되지 않았으며, 2020년 성폭력처벌법 제14조의 2¹⁾가 신설된 것을 시초로, 최근에는 정보통신망법의 일부 법조항이 개정되었다²⁾. 다행히 이전에 비하여는 딥페이크 관련 입법논의가 꽤 진행되고 있으나, 법률신

1) 성폭력범죄의 처벌 등에 관한 특례법 제14조의2(허위영상물 등의 반포등)가 2020.3.24. 신설되어 2020.6.25.부터 시행되었다.

2) 개정된 정보통신망법에서는 과학기술정보통신부장관 또는 방송통신위원회로 하여금 딥페이크 관련 기술에 관한 시책을 마련하도록 하였고(정보통신망법 제4조 제2항 7의2

설안 및 개정안에 대한 추가적인 논의가 계속 필요하다.

현재 진행되고 있는 입법논의 및 정책을 구체화하고, 딥페이크 대응과 규제에 더욱 효과적으로 적용할 수 있는 신설안 또는 개정안을 마련하기 위하여는, 딥페이크 관련 기술 및 해외 입법 현황 조사가 선행되어야 한다. 또한 딥페이크 관련 법적 이슈 및 기존에 마련되어 있는 국내 규제체계를 파악하여 규제공백을 메우고 규제 사각지대를 해소할 필요성이 있다.

본 연구에서는 딥페이크 기술 동향, 해외 입법 동향을 살펴보고, 국내 딥페이크 입법 및 제도 현황을 분석함으로써, 딥페이크 기술의 발전으로 인한 부작용을 예방하고, 딥페이크 기술로 인한 피해자를 보호하는 방향의 입법 및 정책을 제안하고자 한다.

호), 일정규모 이상의 정보통신서비스 제공자로 하여금 딥페이크 기술로 생성된 음란물의 유통을 방지하기 위한 책임자를 지정하고(동법 제44조의 9), 불법촬영물 등의 유통 방지와 관련된 각종 사항에 대한 보고서 작성 및 제출 의무를 부여하였다(동법 제64조의5). 위 개정법률안은 2020. 6. 29. 공포되어 2020. 12. 10.부터 시행예정이다.

제2절 연구의 목표 및 내용

본 연구의 목적은 딥페이크 기술과 관련된 기술동향 및 해외 입법, 정책 동향을 파악함으로써 이를 국내 입법 및 정책에 반영하고, 딥페이크 기술의 발전으로 인한 사회적 역기능 저하, 딥페이크로 인한 형사처벌 및 피해자의 구제를 종합적으로 고려하여 균형있는 입법개선 방향 및 정책안을 제시하는 것이다.

구체적인 연구의 내용은 다음과 같다.

- 딥페이크 기술 관련 기술 개발 동향 및 해외 입법 등 대응 동향 분석
 - 해외 및 국내의 최신 딥페이크 기술 동향 조사·분석
 - 해외 주요국의 딥페이크 기술 관련 입법 및 정책 대응 조사·분석
- 딥페이크 기술 관련 입법 개선방안 제시
 - 국내 딥페이크 기술 관련 입법 현황 조사·분석
 - 국내 딥페이크 기술 관련 법령 제·개정 방향 제시
- 딥페이크 기술 관련 제도 개선방안 제시
 - 국내 딥페이크 기술 관련 제도 현황 조사·분석
 - 국내 딥페이크 기술 관련 제도 개선 및 근거규정 마련 방안 제시
- 딥페이크 기술 관련 규제체계 전반 등을 논의하기 위한 범부처 협의체 구성 제시
 - 딥페이크 관련 범부처협의체의 업무와 운영

위와 같이 기술·입법·제도를 동시에 살펴봄으로써, 국내 입법과 제도 현황상 딥페이크 기술을 다루는데에 부족함이 없는지 살피고, 향후 딥페이크 기술에 대한 효과적인 규제를 위한 입법 및 제도 개선방안을 제안하고자 한다.

제2장 딥페이크 기술 관련 기술 및 해외 입법 등 대응 동향 분석

제1절 딥페이크 관련 기술 동향

1. 딥페이크(deepfake)의 정의

딥페이크(deepfake)는 딥러닝(Deep learning³⁾)과 페이크(fake)의 합성어로, 합성 대상의 얼굴 이미지를 원본 영상에 합성하여 합성 대상자가 원본 영상과 같은 행동이나 말을 하는 것처럼 보이는 동영상을 생성해내는 기술이다.

구체적으로 딥페이크 기술은 사람을 대상으로 한 영상에 인공지능 기술을 이용하여 타인의 얼굴이나 신체 부위의 이미지를 중첩하거나 결합함으로써 일반인이 합성 여부를 확인하는 것이 사실상 불가능한 가공의 영상을 만드는 기술이라는 의미로 널리 쓰이며, 간단히는 인공지능 기반 기술로 만들어진 진짜처럼 보이는 가짜 동영상, 음성파일 등을 지칭한다.

이렇듯 딥페이크 기술은 임의의 입력 데이터를 학습을 통하여 사용자가 원하는 방향으로 변화시키는 기술이다. 딥페이크 기술을 통하여 사람의 얼굴 전체를 대체하거나 특정한 요소를 골라서 변형시킬 수도 있다. 또한 딥페이크 기술은 시각데이터 뿐만 아니라 다른 종류의 데이터에도 적용할 수 있다. 딥페이크 기술을 사람의 목소리에 적용하는 경우 말의 빠르기나 억양, 사투리 사용 유무 등의 특성은 그대로 유지되 목소리만 다른 사람의 것으로 치환할 수 있다. 딥페이크 기술을 사람의 손 글씨에

3) 딥러닝(Deep learning)은 컴퓨터가 사람처럼 생각하고 배울 수 있도록 하는 기술을 뜻한다. 기계학습의 한 분야이나, 기계학습은 컴퓨터에게 다양한 정보를 가르치고 학습한 결과에 따라 컴퓨터가 새로운 것을 예측하는 반면, 딥러닝은 인간의 가르침이라는 과정 없이도 스스로 학습하고 미래의 상황을 예측하는 것이다.

적용하는 경우 마치 다른 사람이 직접 쓴 것처럼 보이는 효과를 낼 수도 있다.

이전의 합성 영상들은 완벽한 합성이 불가능에 가까워 육안으로 조작사실을 판명할 수 있거나, 합성판별 기술로서 조작영상인지를 구별해낼 수 있었다. 딥페이크 기술은 얼굴에 나타나는 표정이나 움직임 분석하여 인공지능 기술을 통해 합성하기 때문에 기존의 합성기술과 달리 조작사실을 매우 인지하기 어렵다.

이렇듯 딥페이크 영상은 그것이 딥페이크 기술을 활용한 영상인지를 판별하기가 극도로 어렵기 때문에 사회적으로 악용될 가능성이 더욱 높고, 이를 규제해야 한다는 목소리가 높아진 것이다.

2. 딥페이크 생성 기술의 발전

2.1. 딥페이크 생성 기술 개요

딥페이크는 기술은 주로 오토인코더⁴⁾(Autoencoder) 또는 생성적 적대 신경망(GAN: Generative Adversarial Network)을 핵심으로 한다. 최초의 딥페이크 얼굴은 오토인코더를 사용하여 만들어으나, 더 발전된 학습 모델인 적대적 생성 신경망이 최근 적용되고 있으며, 향후 오토인코더보다는 적대적 생성 신경망이 보다 광범위하게 사용될 것으로 전망된다.

2.1.1. 오토인코더(Autoencoder) 기술

오토인코더(Autoencoder)는 입력 데이터를 인코더(Encoder)를 이용하여 낮은 차원의 은닉 공간(latent space) 임베딩(embedding)⁵⁾한 뒤 이를 다시 디코더(Decoder)⁶⁾를 이용

4) 입력된 데이터를 다음 단계에서 사용할 수 있도록 부호화하는 장치를 뜻한다.

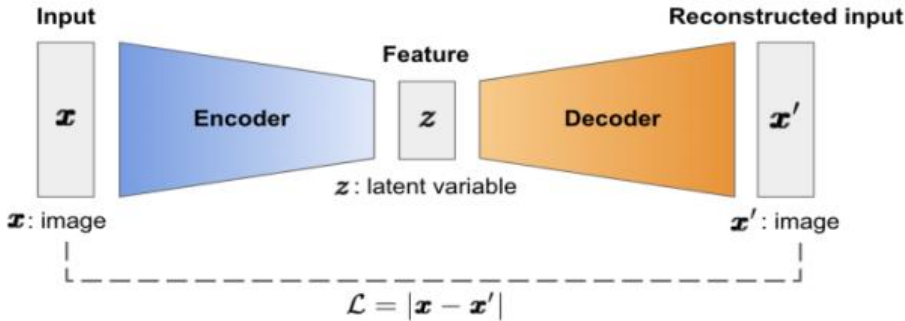
하여 원래 데이터로 복원하는 기능을 가진 신경망을 의미한다. 완벽한 오토인코더는 입력 데이터를 똑같이 복원할 수 있어야하기 때문에 입력과 출력의 차이를 손실 함수(loss function)로 정의하고 이를 최소화도록 학습을 수행한다. 이러한 신경망이 제안된 이유는 레이블(label)을 갖지 않은 데이터만으로도 데이터의 표현법(representation)을 학습할 수 있기 때문이다.

학습이 완료된 오토인코더는 입력 데이터를 낮은 차원의 은닉공간 내의 벡터(vector)⁷⁾로 표현하고 이 정보만으로 디코더를 사용하여 원래 입력 데이터를 복원하게 되는데, 이는 은닉 공간에 임베딩(embedding)된 벡터가 원래 영상에 대한 정보를 대부분 가지고 있기 때문에 가능하다. 따라서 은닉 공간에 표현된 벡터는 입력 데이터를 잘 표현하고 있다고 할 수 있고 이를 분류기와 연결하면 분류 성능을 높일 수 있는 것이다.

아래 그림과 같이 오토인코더는 인코더와 디코더를 대칭적으로 구성하고 입력데이터와 출력데이터의 차를 줄여나가는 방법으로 학습이 진행된다. 딥페이크에서는 오토인코더를 데이터를 효과적으로 표현하여 분류 작업을 수행하는 용도만으로 사용하지 않고, 표현된 데이터를 이용하여 입력 영상을 사용자가 원하는 형태로 변형시킬 수 있는 알고리즘으로 진화시켰다.

-
- 5) 이산변수(discrete variable)가 연속적인 숫자로 구성된 벡터(vector)로 표현될 수 있도록 하는 것을 뜻한다.
 - 6) 인코더의 역기능을 가지는 것을 뜻한다.
 - 7) 크기와 방향을 가지는 양을 뜻한다. 위치, 속도, 힘 등과 같은 물리량을 나타내는데 사용된다.

[그림 2-1] Autoencoder의 구조



딥페이크를 이용하여 사람의 얼굴을 다른 사람의 얼굴로 변경하는 기술은 여러 개의 오토인코더를 동시에 학습함으로써 이루어진다. A라는 사람의 얼굴을 B라는 사람으로 바꾸고 싶다면, 가장 중요한 과정 가운데 하나가 A와 B의 얼굴에 대한 많은 양의 데이터를 수집하는 것이다. 데이터를 수집하고 난 후에 A와 B의 얼굴을 복원하는 오토인코더를 각각 학습시킨다. 이때, 두 개의 오토인코더의 인코더 부분은 파라미터(parameter)⁸⁾들을 공유하고, 디코더는 사람마다 별도로 학습시킨다. 즉 공통의 인코더로 얼굴 영상을 낮은 차원의 은닉 공간에 임베딩 한 뒤 각 사람별로 디코딩함으로써 원래 얼굴을 복원하는 신경망을 학습시키는 것이다.

오토인코더를 학습할 때는 입력 얼굴과 출력 얼굴의 차이가 최소화되도록 손실 함수(loss function)를 정의하고 이 손실 함수(loss function)를 최소화시킨다. 이 때, 복원된 얼굴이 보다 자연스럽게 보이고 시맨틱(semantic)한 정보를 잘 보존하게 하기 위하여 적대적(adversarial) 및 인지적(perceptual) 손실을 손실 함수(loss function)에 추가하기도 한다⁹⁾. 여기서 적대적 손실이란 복원된 얼굴이 자연스럽게 보이도록 복원된 영상이 사람의 얼굴같이 보이는지 아닌지를 판별할 때 발생하는 오차를 의미하고, 인지

8) 각 변수 사이의 함수관계를 정하기 위해서 이용되는 또 다른 변수를 뜻한다.

9) Keras-VGGFace: VGGFace implementation with Keras framework. Retrieved from <https://github.com/rcmalli/keras-vggface>

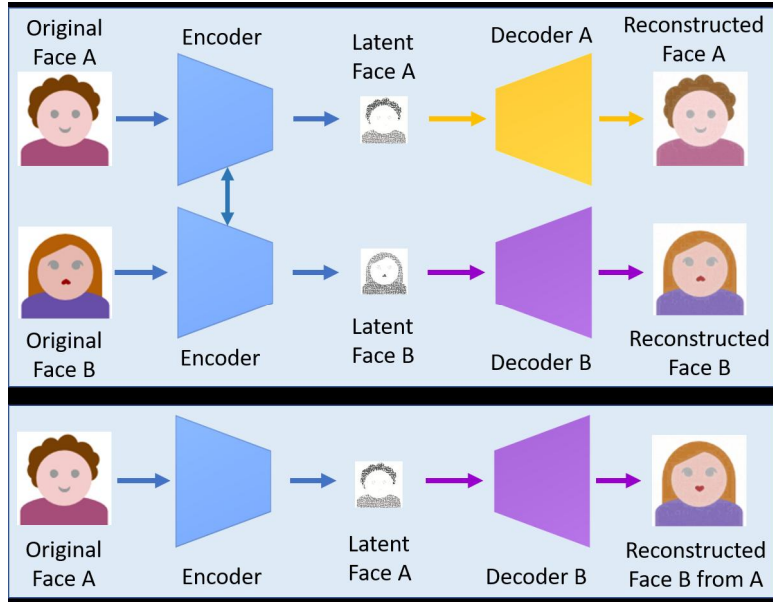
적 손실은 복원된 얼굴이 입력 얼굴이 유사한 두 개의 벡터로 표현되는지를 확인하기 위하여 그 차이를 계산한 것을 의미한다.

이와 같이 학습된 신경망을 가지고 있을 때, A에 해당하는 얼굴을 입력하여 인코더로 임베딩한 뒤 B의 얼굴을 복원하는 디코더로 디코딩하면 입력 얼굴의 다른 특징은 그대로 보존하면서 얼굴의 주인만 B로 바뀐 결과를 얻을 수 있다. 반대로 B에 해당하는 얼굴을 인코딩한 뒤 A에 대한 디코더로 디코딩 하면 A에 대한 얼굴을 얻을 수 있다. 만약 두 명 이상의 다른 사람에 대한 딥페이크를 수행하기 위해서는 각각의 사람마다 별도의 오토인코더 학습이 필요하고 추론 시에는 원하는 인코더와 디코더 쌍을 이용하여 딥페이크를 수행할 수 있다.

이와 같은 방식으로 딥페이크를 구현을 할 경우, 영상 내에 얼굴뿐만 아니라 다른 부분도 존재하기 때문에 실제로는 오토인코더를 이용하여 얼굴을 변형시키는 작업 이외의 과정이 필요하다. 예를 들면 입력 이미지에서 얼굴 부분을 검출해야하고, 그 얼굴을 딥페이크를 이용하여 다른 사람의 얼굴로 변형시킨 뒤에는 출력 이미지와 입력 얼굴을 변형시킨 결과를 자연스럽게 결합시키는 과정이 필요하다. 이러한 과정들은 딥페이크와는 관련이 없는 별도의 알고리즘이 필요한데, 이 부분이 딥페이크로 만들어진 영상이 부자연스러워 보이는 원인이 되기도 한다.

<그림삽입을 위한 여백>

[그림 2-2] 오토인코더(Autoencoder) 방식을 사용한 딥페이크 영상 제작



자료 : T. T. Nguyen, C. M. Nguyen, D. T. Nguyen, D. T. Nguyen, and S. Nahavandi, "Deep learning for deepfakes creation and detection," arXiv preprint arXiv:1909.11573, 2019

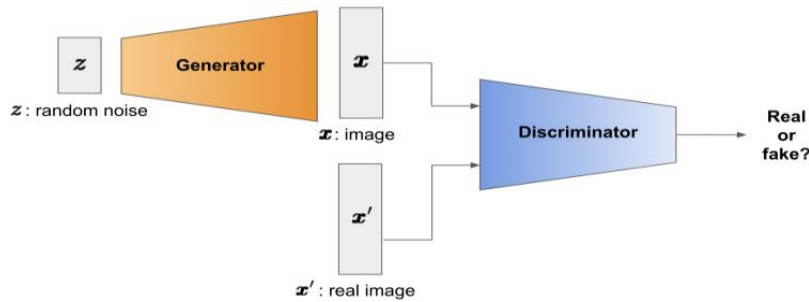
2.1.2. 적대적 생성 신경망(GAN) 기술

생성적 적대 신경망GAN(Generative Adversarial Network) 기술(이하 'GAN기술')은 이미지의 진위여부를 판별하는 '감별자 알고리즘(식별모델)'과 이미지를 만들어내는 '생성자 알고리즘(생성모델)'으로 구성된다.

생성모델은 임의의 노이즈 벡터가 주어질 때 영상을 생성하는 역할을 하고, 식별모델은 주어진 입력 영상이 실제로 존재하는 영상(real image)인지 아니면 생성모델이 생성한 영상(fake image)인지 구별한다. 생성모델과 식별모델은 같이 연결되어 있다.

영상 데이터를 사용하는 적대적 생성 신경망에서는 일반적으로 생성모델과 식별모델 모두 컨볼루션 신경망(convolutional neural network; CNN)을 주로 사용한다.

[그림 2-3] 적대적 생성 신경망의 구조



적대적 생성 신경망의 학습 과정을 간단하게 설명하면 다음과 같다. 식별모델이 입력으로 주어진 영상이 진짜인지 가짜인지 쉽게 구별을 할 수 있으면 생성모델을 업데이트 시키고, 판별을 하지 못하면, 즉 식별모델의 예측이 틀리면 식별모델을 업데이트 한다. 이와 같이 생성모델과 식별모델이 서로 경쟁하는 방식의 학습이 마무리되면 생성모델은 고품질의 영상을 생성할 수 있게 되고, 분별 신경망은 생성된 영상이 진짜인지 가짜인지 잘 구별할 수 있게 된다. 학습의 목표는 생성모델이 식별모델을 속이는 것이므로 생성모델이 실제 영상과 거의 유사한 품질의 영상을 만들 수 있게 되면 학습이 종료된다.

이러한 개념을 사용하면 얼굴의 신원이 변경된 딥페이크 기술을 구현할 수 있는데, 그 가능성을 보여준 가장 대표적인 예가 CycleGAN이다¹⁰⁾. CycleGAN에서는 두 사람에 대한 데이터셋(dataset) 내의 각 영상의 대응관계를 모르더라도 한 사람의 영상을 다른 사람의 영상으로 바꿀 수 있는 신경망으로써 논문에서 제안된 기술을 개선하여

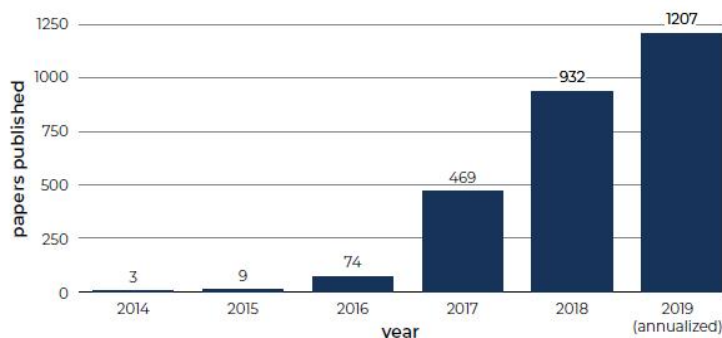
10) J.-Y. Zhu*, T. Park*, P. Isola, A. A. Efros: Unpaired Image-to-Image Translation using Cycle-Consistent Adversarial Networks. ICCV 2017

주로 겉모습(appearance)만 변화시키는 한계를 넘어 시맨틱한 정보까지도 원하는대로 변경될 수 있음을 보여주었다. 또한 적대적 손실 함수를 사용함으로써, GAN을 직접 사용하지 않더라도, 변형된 영상이 자연스럽게 보이도록 하는 노력도 계속되었다. 한편 GAN을 사용하면 오토인코더로는 수행하기 어려운 작업들도 가능해지는데 어떤 사람이 특정한 말을 한 것처럼 입술모양까지 유사하게 동영상상을 조작할 수 있는 립싱크(lip sync)가 대표적이다.

생성모델에는 오토인코더(Autoencoder) 기술이 적용될 수 있다. 이러한 방식으로 오토인코더(Autoencoder)와 GAN 기술을 동시에 활용하여 딥페이크 영상의 정밀도를 더욱 높이기도 한다¹¹⁾.

GAN 기술에 대한 연구는 2014년 이후 서서히 증가하기 시작하여 2016년부터 본격적으로 증가하였고, 2019년 9월 기준 1,207건에 이르는 연구가 이루어진 것으로 파악된다(arXiv 게재 수 기준¹²⁾).

[그림 2-4] GAN 기술에 대한 연구 수 증가 (arXiv 게재 수 기준)



한편 GAN 기술을 활용한 오픈 소스 프로그램이 널리 배포되면서 딥페이크 기술을 활용한 영상 제작이 활성화 되고 있다.

11) Faceswap-GAN. 배포: <https://github.com/shaoanlu/faceswap-GAN>

12) arXiv는 코넬대학교가 운영하는 과학 및 수학 연구 논문의 온라인 아카이브(기록보관소)이다.

<표 2-1> 주요 딥페이크 오픈 소스

프로젝트 명	특징	웹사이트
Faceswap	2쌍의 Encoder-Decoder를 사용 Encoder의 Parameter를 공유함	https://github.com/deepfakes/faceswap
Faceswap -GAN	Autoencoder에 GAN을 통합함	https://github.com/shaoanlu/faceswap-GAN
DeepFace Lab	Faceswap을 변형하여 만들어짐 다양한 얼굴 추출 알고리즘을 지원	https://github.com/iperov/DeepFaceLab
DFaker	Keras 라이브러리 사용	https://github.com/dfaker/df
DeepFake -tf	DFaker와 유사하나 tensor-flow 라이브러리 기반으로 제작됨	https://github.com/StromWin/DeepFake-tf

위의 딥페이크 오픈 소스 도구들 가운데 다수는 학술적 목적으로 프로그램 및 소스 코드를 배포하는 것이 아니라 일반 사용자들이 편리하게 사용할 수 있도록 인터페이스가 구성되어 있고 자세한 튜토리얼이 마련되어 있는 경우도 있다.

2.2. 딥페이크 생성 기술 동향

딥페이크 기술은 2017년 말, 미국의 소셜 커뮤니티 사이트인 레딧(Reddit)의 한 유저인 'deepfakes'가 연예인들의 얼굴을 합성한 음란 영상을 업로드하면서 알려지기 시작했다¹³⁾. 'deepfakes'는 오토인코더(Autoencoder) 기술을 적용하여 합성 영상을 제작할 수 있는 프로그램인 FakeApp을 개발했고, 현재까지도 이를 무료로 배포하고 있다¹⁴⁾. 음란 영상 이외에 미국 영화배우 니콜라스 케이지(Nicolas Cage)의 얼굴을 이용한 다양한 합성 사진 및 동영상도 동시에 공유되었다.

13) BBC 뉴스, Deepfakes: What are they and why would I make one?,
<https://www.bbc.co.uk/bitesize/articles/zflkwcqt>

14) FakeApp 다운로드 페이지 (<https://www.malavida.com/en/soft/fakeapp/>)

[그림 2-5] 딥페이크 기술을 이용한 합성 예



자료 : Night W. (2018.8.7)

초기 딥페이크 기술은 해상도의 제한이 있거나 영상 제작을 위한 계산 시간이 오래 걸리는 등 문제가 있었으나 발전을 거듭하여 실시간으로 영상 속 사람의 표정이나 움직임 변형하는 기술도 개발되었다.

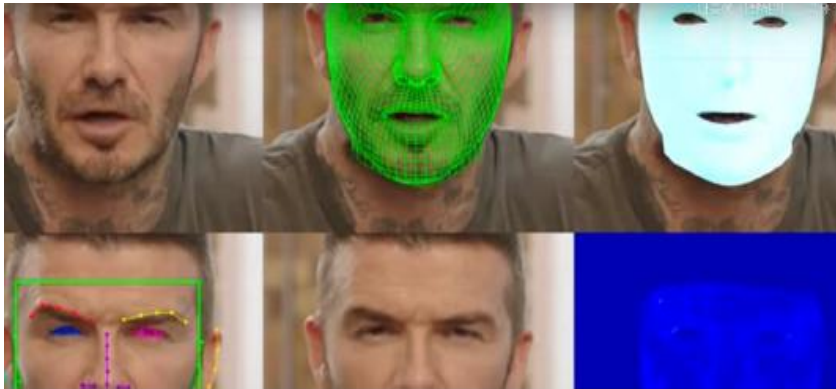
[그림 2-6] 실시간 딥페이크 합성



자료 : Justus Thies 웹사이트(<https://justusthies.github.io/posts/headon/>)

초기 딥페이크 기술은 원본 영상을 새로 촬영한 후 원본 영상 위에 새로운 영상 또는 이미지를 중첩시키는 방식으로 제작되었으나, 최근에는 새로 원본영상을 촬영하지 않고 기존 자료만을 편집하여 딥페이크 영상을 제작할 수 있는 기술이 개발되었다. 영국 Synthesia사가 2019. 4. 발표한 유명 축구 선수 데이비드 벅엄(David Beckham)의 말라리아 퇴치 홍보 캠페인 영상이 대표적이다. 해당 영상에서 벅엄은 중국어, 아랍어, 힌디어, 스와힐리어, 요루바어(나이지리아, 토고 지역 아프리카 언어) 등 9개 언어로 말라리아 퇴치 캠페인을 진행한다.

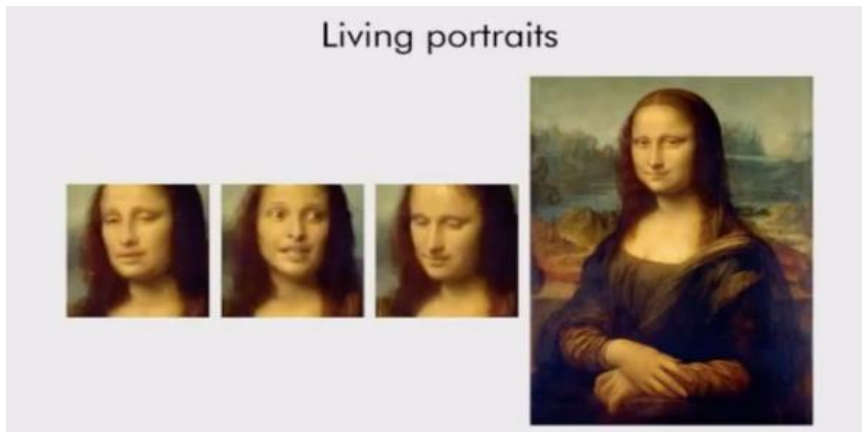
[그림 2-7] 말라리아 퇴치 홍보 캠페인 영상 제작 과정



자료 : Techcrunch(April 25, 2019), "The startup behind that deep-fake David Beckham video just raised \$3M"

또한 초기 딥페이크 기술은 대상 인물의 사진이 대량으로 필요했으나, 최근 1장의 사진을 이용하여 별도의 3차원 리모델링 과정 없이 말하는 얼굴 동영상(talking head videos)을 만들 수 있는 기술이 개발되었다. 삼성전자 러시아 모스크바 AI연구센터가 2019. 5. 발표한 모나리자 동영상이 대표적이다.

[그림 2-8] 삼성전자 AI연구센터가 만든 모나리자 동영상



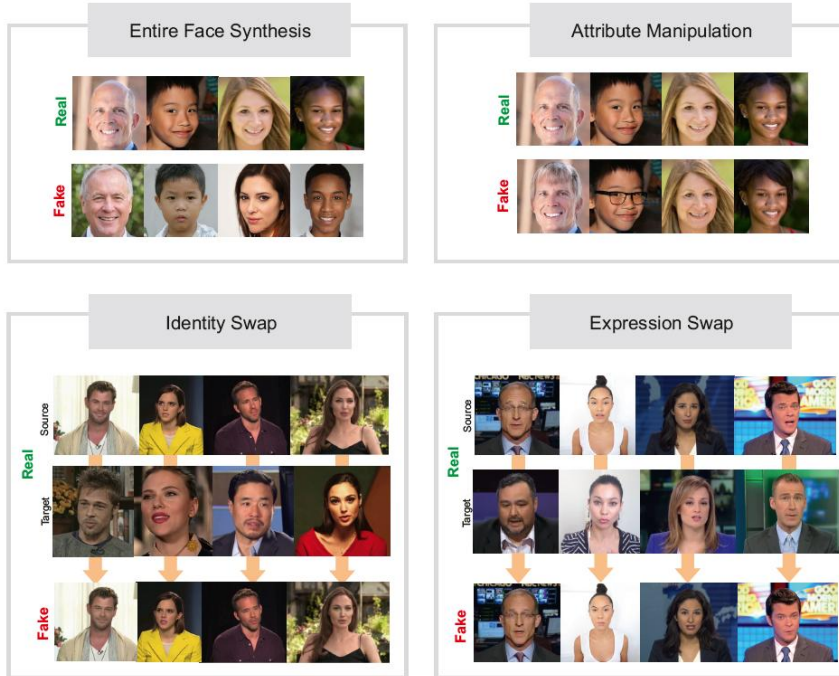
자료 : 이고르 자카로프 유튜브채널¹⁵⁾

딥페이크 기술을 활용하여 실제로 존재하지 않는 사람의 얼굴을 합성(Entire Face Synthesis)하거나 안경이나 머리스타일 같은 일부분을 조작(Attribute Manipulation)하거나 실제 영상의 표정만 변경(Expression Swap)하는 방식도 가능하다. 또한 실시간으로 영상 속 사람의 표정이나 움직임을 변형할 수도 있다.

<그림삽입을 위한 여백>

15) <https://www.youtube.com/channel/UCsxwjK5ELsIXWs62jqBCAbA>

[그림 2-9] 딥페이크 기술 활용 예



자료 : Ruben Tolosana, Ruben Vera-Rodriguez, Julian Fierrez, Aythami Morales, and Javier Ortega-Garcia. "Deepfakes and beyond: A survey of face manipulation and fake detection." arXiv preprint arXiv:2001.00179, 2020.

딥페이크 영상 제작의 원리를 이용하여 음성을 합성하는 기술도 계속하여 발전하고 있다. 2019. 11. 유튜브채널 'Two Minute Papers¹⁶⁾'에서는 5초 분량의 목소리를 참조해 같은 목소리로 말하는 음성파일을 합성하는 기술을 소개하였다¹⁷⁾.

최근 적대적 생성 신경망을 이용하여 생성된 영상의 품질은 놀라울 정도로 빠르게

16) 인공지능 논문을 2분만에 설명해주는 유튜브채널
(<https://www.youtube.com/user/keerozy/videos>)

17) <https://www.youtube.com/watch?v=0sR1rU3gLzQ>

향상되고 있다.

[그림 2-10] 적대적 생성 신경망으로 생성된 영상들의 품질변화



자료 : <https://blog.inten.to/welcome-to-the-simulation-dd0d8cb6534d>

3. 딥페이크 감별 기술의 발전

3.1. 딥페이크 감별 기술의 등장 및 한계

딥페이크 생성 기술이 비약적으로 발전하면서, 딥페이크 감별 기술 또한 함께 발전하고 있다. 초창기에는 딥페이크로 만들어진 영상을 검출하기 위하여 수동으로 영상 내의 부자연스러운 부분이나 일관되지 않은 정보를 찾아내는 피쳐(feature)를 개발하는데 그쳤으나, 최근에는 딥러닝을 이용하여 검출하는 방법이 주로 사용되고 있다. 학습을 통한 딥페이크 검출은 주로 이진 분류(binary classification)기반으로 이루어지는데, 이는 입력 영상이 실제 영상인지 아니면 딥페이크로 조작된 영상인지 두 개의 클래스로 구분하는 방법을 의미한다. 하지만 이러한 방법은 각각의 클래스에 대하여 많은 수의 데이터를 수집해야 모델을 학습할 수 있는 단점이 있다. 딥페이크의 주요 용

도는 영상 내 사람의 신원을 바꾸는 것이기 때문에 얼굴 인식 알고리즘을 통해서도 구분이 가능할 수 있으나 아쉽게도 FaceNet과 같은 얼굴 인식 알고리즘은 딥페이크 얼굴 검출에 취약한 것으로 나타났다¹⁸⁾.

[그림 2-11] 실제 영상(좌)과 조작된 영상(우)의 비교



자료 : Zhou et al. (2017)

또한 립싱크(Lip synching)를 활용한 방법¹⁹⁾²⁰⁾이나 서포트 벡터 머신(Support Vector Machine; SVM)이라는 분류기 기반 영상 품질 평가 알고리즘을 이용한 방법²¹⁾ 또한 검출 성능이 상당히 낮은 것으로 보고되고 있다.

3.2. 딥페이크 감별 기술 동향

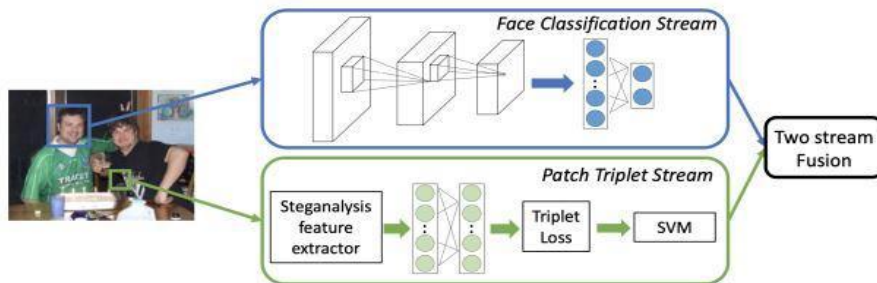
-
- 18) F. Schroff, D. Kalenichenko, J. Philbin: FaceNet: A unified embedding for face recognition and clustering. CVPR 2015
- 19) J. S. Chung, A. Senior, O. Vinyals, A. Zisserman: Lip reading sentences in the wild. CVPR 2017
- 20) S. Suwajanakorn, S. Seitz, I. Kemelmacher-Shlizerman: Synthesizing Obama: learning lip sync from audio. ACM Transactions on Graphics (TOG), 36(4), 2017
- 21) D. Wen, H. Han, A. K. Jain: Face spoof detection with image distortion analysis. IEEE Transactions on Information Forensics and Security, 10(4), 746-761, 2015

딥페이크 영상의 검출은 주로 테스트 대상 영상으로부터 특징을 추출하고 이진 분류를 수행함으로써 이루어진다. 이진 분류기의 입력이 되는 특징은 사람이 디자인하기도 하지만 최근 들어서는 인공 신경망을 이용하는 경우가 훨씬 빈번하다.

뉴욕 알바니주립대학 시웨이 류(Siwei Lyu) 교수 연구진은 딥페이크를 이용하여 만들어진 얼굴 영상의 머리의 위치와 자세(head pose)를 이용하여 이 영상이 얼마나 실제와 같이 자연스러운지를 SVM(서포트 벡터 머신, Support Vector Machine)을 이용하여 판별하는 방식으로 딥페이크 영상을 검출하고자 하였다.

투 스트림(two-stream) 신경망을 이용한 딥페이크 영상 검출 알고리즘을 제안한 기술도 있다. 두 개의 스트림 가운데 하나는 얼굴을 분류하는 모듈로 얼굴 영상이 진짜인지 아니면 가짜인지 판별하고, 패치 트리플릿 스트림(patch triplet stream)은 패치가 같은 영상 내에 존재하는 것인지 아니면 다른 곳에서 가져온 것인지(혹은 조작된 것인지) 판별하는 역할을 한다²²⁾. 아래 [그림 2-12]에서 위쪽이 얼굴이 진짜인지 가짜인지를 구별하는 부분을 담당하고, 아래쪽이 각 패치가 이미지 내에서 자연스럽게 존재하는 것인지 조작된 것인지를 판별한다.

[그림 2-12] 투 스트림 신경망을 이용한 딥페이크 검출 알고리즘

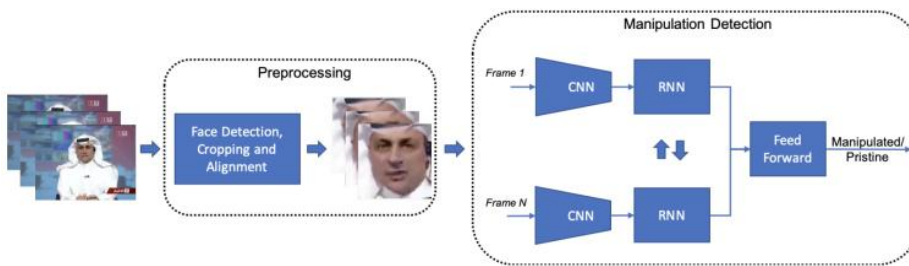


자료: Zhou et al. (2017)

22) P. Zhou, X. Han, V. I. Morariu, L. S. Davis: Two-Stream Neural Networks for Tampered Face Detection. CVPR Workshops 2017

딥페이크 동영상 내에 조작된 부분의 시간적 일관성이 떨어진다는 점에 착안하여 CNN(컨볼루션 신경망, convolutional neural network; CNN)과 RNN(재귀적 신경망, Recurrent Neural Network; RNN)을 동시에 사용하여 딥페이크 동영상 검출에 특화된 시공간적 표현법을 개발한 기술도 있다²³⁾. 이 알고리즘에서는 [그림 2-13]과 같이 우선 동영상의 매 프레임으로부터 얼굴을 검출하고 잘라내어 위치를 잘 맞춰 놓은 뒤 각 프레임에서 검출된 얼굴을 CNN에 통과시켜 각 얼굴의 특징 벡터를 얻고 이를 재귀적 신경망(RNN)의 각 셀(cell)에 입력한 결과를 토대로 최종적으로 이진분류를 통해 진짜 영상인지 가짜 영상인지 판별한다.

[그림 2-13] CNN과 RNN을 사용하여 딥페이크 동영상을 검출하는 알고리즘을 도식화한 예



자료: Sabir et al. (2019)

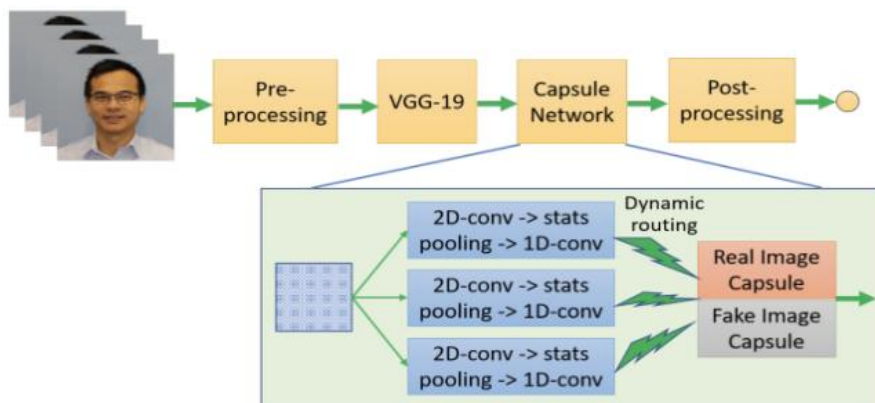
독일 뉘른버그 대학 마크 스태밍어(Marc Stamminger) 교수 연구진은 눈, 이, 얼굴의 경계 부분의 특징들의 일관되지 않은 점이나 조명 혹은 기하학적 부조화 등을 이용하

23) E. Sabir, J. Cheng, A. Jaiswal, W. AbdAlmageed, I. Masi, P. Natarajan: Recurrent Convolutional Strategies for Face Manipulation Detection in Videos. CVPR Workshops 2019

여 딥페이크를 검출하기도 하였다. 연구진은 로지스틱 회귀분석(logistic regression)이나 작은 신경망을 학습시켜 최종적으로 딥페이크 동영상상을 구별했다.

동경대 이사오 이치젠(Isao Echizen) 교수 연구진에서는 조작된 딥페이크 동영상상을 캡슐 신경망²⁴⁾을 이용하여 검출하고자 하였다. 이 기술은 [그림 2-14]와 같이 3개의 캡슐 모듈의 출력을 진짜와 가짜 영상으로 나누는 캡슐로 라우팅(routing)²⁵⁾하는 동적 라우팅 알고리즘을 제안하였다.

[그림 2-14] 캡슐 신경망 이용하여 조작된 동영상상을 검출하는 방법의 개요



자료: Nguyen et al. (2019)

24) S. Sabour, N. Frosst, G. E. Hinton: Dynamic routing between capsules. NIPS 2017

25) 목적지까지 갈 수 있는 여러 개의 경로 중 한 가지 경로를 설정하는 것을 뜻한다.

<표 2-2> 딥페이크 감별 기술

감별기술	주체	출처
입술과 목소리의 불일치를 이용한 감별	스위스 Idiap 연구소 세바스티안 마르셀 연구진 (Sébastien Marcel)	P. Korshunov and S. Marcel, "Deepfakes: a New Threat to Face Recognition? Assessment and Detection," arXiv preprint arXiv:1812.08685, 2018.
눈 색깔, 반사광, 눈이나 치아의 미세한 주름 등을 이용한 감별	독일 뉘른버그 대학 마크 스태밍어 교수 (Marc Stamminger)	F. Matern, C. Riess, and M. Stamminger, "Exploiting Visual Artifacts to Expose DeepFakes and Face Manipulations," in Proc. IEEE Winter Applications of Computer Vision Workshops, 2019
머리의 움직임에 이용한 감별	뉴욕 알바니주립대학 시웨이 류 교수 (Siwei Lyu)	X. Yang, Y. Li, and S. Lyu, "Exposing Deep Fakes Using Inconsistent Head Poses," in Proc. International Conference on Acoustics, Speech and Signal Processing, 2019.
얼굴 근육의 움직임을 이용한 감별	다트머스 대학 해니 파리드 교수 (Hany Farid)	S. Agarwal and H. Farid, "Protecting World Leaders Against Deep Fakes," in Proc. IEEE/CVF Conference on Computer Vision and Pattern Recognition Workshops, 2019.
사람의 눈 깜박임 패턴을 이용한 감별	건국대학교 김기천 교수	T. Jung, S. Kim, and K. Kim, "DeepVision: Deepfakes Detection Using Human Eye Blinking Pattern," IEEE Access, vol. 8, pp. 83 144-83 154, 2020.
공개된 데이터베이스에 딥러닝을 적용하여 실제 영상과 가짜 영상을 구별하는 감별	동경대 이사오 이치젠 교수 (Isao Echizen)	H. Nguyen, F. Fang, J. Yamagishi, and I. Echizen, "Multi-task Learning For Detecting and Segmenting Manipulated Facial Images and Videos," arXiv preprint arXiv:1906.06876, 2019.

최근 마이크로소프트는 2020. 9. 1. "마이크로소프트 비디오 어센터케이터(Microsoft

Video Authenticator)"라는 딥페이크 식별기술을 발표했다. 이 마이크로소프트 비디오 어센터케이터는 스틸 사진이나 비디오를 분석하여 미디어가 인위적으로 조작되는 확률 또는 신뢰 점수를 제공할 수 있다. 동영상의 경우 재생되는 동안 각 프레임에서 이 비율을 실시간으로 제공해, 사람의 눈으로 감지할 수 없는 딥페이크 기술로 편집이 이뤄졌는지 여부를 판정하고 '신뢰 점수'를 계산해 딥페이크가 사용됐는지 알 수 있도록 표시해준다.

이 기술에는 두 가지 요소가 있다. 첫 번째는 콘텐츠 제작자가 콘텐츠에 디지털 해시와 인증서를 추가할 수 있도록 하는 마이크로소프트 Azure에 내장된 툴이다. 해시와 인증서는 콘텐츠가 온라인에서 어디로 이동하든 메타데이터로서 콘텐츠와 함께 유지된다. 두 번째는 브라우저 확장자 또는 다른 형태로 존재할 수 있는 인증서를 확인하고 해시를 일치시키며, 콘텐츠가 진품이고 변경되지 않았음을 사람들에게 높은 정확도로 알려주고, 누가 그것을 생산했는지에 대한 세부사항을 제공한다.

실제로 마이크로소프트가 공개한 데모 영상엔 딥페이크가 감지될 경우 빨간색 글자와 함께 특정 퍼센트로 표시된다. 딥페이크의 미묘한 페이딩 또는 그레이 스케일 요소의 혼합 경계를 감지하여 작동한다. 이 기술은 원래 마이크로소프트의 Responsible AI 팀과 마이크로소프트의 AETHER (Ethics and Effects in Engineering and Research) 위원회와 협력하여 마이크로소프트 리서치에서 개발했다.

3.3. 딥페이크 감별 기술을 위한 데이터베이스 구축

한편, 딥페이크 영상 감별 기술의 발전을 위해 여러 주체들이 실제 영상과 딥페이크 알고리즘을 이용해 생성한 가짜 영상을 제공하는 데이터베이스를 구축하여 제공하고 있다.

구글에서는 조작되지 않은 영상, 그래픽 알고리즘을 이용한 합성영상 및 딥페이크 알고리즘을 이용한 영상을 포함하는 데이터베이스인 페이스포렌식(FaceForensics++)를 제공하고 있다²⁶⁾

구글은 페이스포렌식(FaceForensics++)을 지속적으로 업데이트 하고 있는데, 2019. 9. 23.에는 배우들을 섭외하여 새로이 제작한 실제 영상과 정교한 딥페이크 알고리즘을 적용하여 생성한 가짜 영상을 포함하는 딥페이크디텍션(Deep Fake Detection Dataset)을 추가하였고²⁷⁾, 2020. 7. 15.에는 기존 기술로 감별하기 어려운 알고리즘인 페이스시프터(FaceShifter)를 적용한 데이터²⁸⁾를 추가하였다²⁹⁾.

마이크로소프트 비디오 어센터케이터는 지난해 8월에 아카이브를 통해 공개된 'FaceForensics ++ : 조작 된 얼굴 이미지 감지 학습(FaceForensics++: Learning to Detect Manipulated Facial Images- 다운)'의 공개 데이터셋을 사용하여 만들어졌다. 또한 지난해 12월부터 지난 3월 31일까지 총 상금 100만 달러 규모로 개최된 페이크 검출 챌린지(DFDC) 데이터셋에서 실증 테스트를 받았다³⁰⁾.

페이스북은 2019. 12.부터 2020. 3.까지 마이크로소프트, 아마존 및 MIT와 협력하여 DFDC(The Deepfake Detection Challenge)라는 딥페이크 영상 감별 대회를 개최하였고, 대회에 사용된 데이터베이스³¹⁾ 및 우승자인 셀림 세이베로프의 딥페이크 감별 모델의 소스코드³²⁾는 현재 공개되어 있다.

뉴욕 알바니주립대학의 시웨이 류 교수 연구진은 지난 2019년 Celeb-DF라는 데이터베이스를 공개한 바 있다³³⁾.

26) A. Rössler, D. Cozzolino, L. Verdoliva, C. Riess, J. Thies, and M. Nießner, "FaceForensics++: Learning to Detect Manipulated Facial Images," in Proc. IEEE/CVF International Conference on Computer Vision, 2019.

27) <https://ai.googleblog.com/2019/09/contributing-data-to-deepfake-detection.html>

28) <https://lingzhili.com/FaceShifterPage/>

29) <https://github.com/deepfakes/faceswap>

30) <https://www.aitimes.kr/news/articleView.html?idxno=17581>

31) <https://ai.facebook.com/datasets/dfdc/>

32) https://github.com/selimsef/dfdc_deepfake_challenge

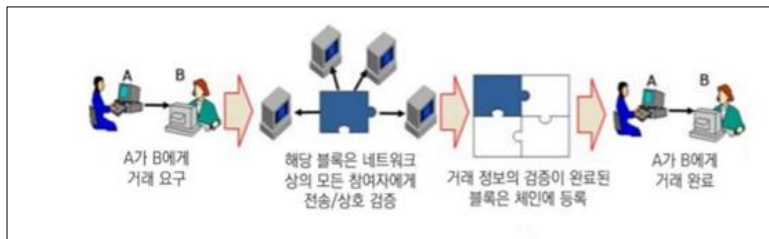
33) Y. Li, X. Yang, P. Sun, H. Qi, and S. Lyu, "Celeb-DF: A Large-Scale Challenging Dataset for DeepFake Forensics," in Proc. IEEE/CVF Conference on Computer Vision and Pattern Recognition, 2020

3.4. 블록체인을 이용한 딥페이크 감별

블록체인이란 P2P(Peer to Peer) 네트워크를 통해서 관리되는 분산 데이터베이스의 한 형태로, 거래 정보를 담은 장부를 중앙 서버 한 곳에 저장하는 것이 아니라 블록체인 네트워크에 연결된 여러 컴퓨터에 저장 및 보관하는 기술로 다양한 분야에 활용이 가능하다.

블록체인은 분산원장 기술(DLT: Distributed Ledger Technology)이라고도 불리며, 이는 거래 정보를 기록한 원장 데이터를 중앙 서버가 아닌 참가자들이 공동으로 기록 및 관리하는 것을 의미한다. 간단히 말하면 누구나 열람할 수 있는 장부에 거래 내역을 투명하게 기록하고, 여러 대의 컴퓨터에 이를 복제해 저장하는 분산형 데이터 저장기술로 일정 주기로 데이터가 담긴 블록을 생성한 후 이전 블록들을 체인처럼 연결한다는 개념이다. 즉 데이터 거래시 기존방식처럼 거래기록을 집중형 서버에 보관하지 않고, 거래에 참여하는 모두가 데이터를 묶음으로 분산·저장, 연결하는 방식으로 공공거래 장부라고도 부르고, 이 기술을 활용하면 데이터 위조나 변조를 할 수 없어 데이터 신뢰성 및 안정성을 제고할 수 있다³⁴⁾.

[그림 2-15] 블록체인 원리



자료: 국방통합데이터센터

34) 국경완, 「블록체인 기술 및 산업 분야별 적용 사례」, 정보통신기획평가원 주간기술동향, 2019. 6. 12.

이처럼 블록체인은 분산처리와 암호화 기술을 동시에 적용하여 높은 보안성을 확보하는 한편 거래과정의 신속성과 투명성을 특징으로 한다. 보안성의 강화로 해커의 공격과 데이터의 왜곡 그리고 기존 중앙집중 서버방식에서 가장 큰 문제인 디도스 공격을 원천적으로 방어할 수 있다. 보안성이 높고 위·변조가 어렵다는 특성 때문에 데이터 원본의 무결성 증명이 요구되는 다양한 공공·민간 영역에 적용되고 있으며, 새로운 신뢰사회 구현의 기반기술로 주목받고 있는 중이다³⁵⁾.

블록체인은 데이터에 무결성을 보증하기 때문에 데이터조작으로부터 안전하고, 데이터 이력 추적에도 활용될 수 있다. 블록체인의 이러한 특징은 딥페이크 악용에 대응할 수 있다. 콘텐츠의 출처를 블록체인으로 기록하면 콘텐츠를 변형하더라도 진위를 파악할 수 있다. 한 마디로, 콘텐츠에 식별 기술을 덧붙이는 셈이다³⁶⁾.

미국 샌프란시스코의 스타트업 앰버 사에서는 영상이나 이미지가 생성될 때 동시에 해당 영상이나 이미지에 대한 해시(Hash)를 생성한다³⁷⁾. 생성된 해시 데이터는 블록체인에 기록되고 원본 여부를 파악하기 위해 사용된다. 원본 데이터가 변형되면 원본 데이터 정보와 새롭게 생성된 해시값이 블록체인에 다시 기록되어 원본 비교에 활용되는 방식이다. 만약 영상이 변형되면 변형된 영상 테두리에 색을 아래 그림처럼 바꿔 조작된 영상임을 인지하도록 알려준다.

아래 그림은 백악관에서 오바마 전 미국대통령의 발언영상이나, 딥페이크 기술을 활용하여 조작된 영상이다. 기존에는 올라온 영상(좌)은 조작 여부를 육안으로 확인하기 어려운 수준이나, 위 기술을 사용하여 영상(우)을 탐지하면 딥페이크 기술이 사용되었다는 사실이 주황색 영상 테두리로 나타나 쉽게 인식할 수 있다. 이는 일반적인 개인 촬영에서는 활용하기 어렵겠지만, 위 영상처럼 백악관에서 촬영된 경우 등에는

35) 김현수, 권혁준 「보험 산업의 블록체인 활용」, 보험연구원, 2018. 12. 10.

36) <https://www.sciencetimes.co.kr/news/%EB%B8%94%EB%A1%9D%EC%B2%B4%EC%9D%B8%EC%9C%BC%EB%A1%9C-%EB%94%A5%ED%8E%98%EC%9D%B4%ED%81%AC-%EB%8C%80%EC%9D%91%ED%95%A0-%EC%88%98-%EC%9E%88%EC%96%B4/>

37) <https://ambervideo.co/#>

위 기술을 활용하면 원본 영상임을 보장할 수 있다³⁸⁾.

[그림 2-16] 조작된 영상(좌)과 식별 기술을 통해 탐지한 결과(우)



자료: <https://www.buzzfeed.com/>

4. 딥페이크 기술에 대한 평가

4.1. 딥페이크 기술의 유용성

딥페이크를 유용하게 사용할 수 있는 응용례들은 다양하다. 과거에는 모션 캡처(motion capture)와 컴퓨터 그래픽 기술을 결합하여 공상과학 영화나 판타지 영화에 나오는 가상의 캐릭터를 만들거나, 영화 촬영 중 사망한 배우가 등장하는 장면을 찍고, 대역 배우의 얼굴을 원래 배우의 얼굴로 치환하거나, 영화의 진행과 맞지 않는 배우의 나이를 조정하는 등의 다양한 형태의 조작을 수행해 왔는데, 이러한 작업도 딥페이크를 이용하여 훨씬 간단하게 수행할 수 있다.

또한, 영화나 드라마에 등장하는 배우를 가상의 방법으로 시청자가 원하는 사람으로 교체함으로써 완벽히 개인화된 캐스팅이 가능해질 수 있다. 음성을 모사하여 가수

38) 저작권위원회, 「저작권기술 동향」, 2019. 2.

의 목소리를 특정인의 목소리로 치환하여 마치 다른 사람이 부른 노래처럼 들리게 할 수도 있다.

한편, 딥페이크는 의료기술에 이용되어 의학발전에 기여할 수 있다.

4.2. 딥페이크 기술의 문제점과 대책

딥페이크 기술로 제작된 영상은 실제와 구분이 불가능하기 때문에 악용될 가능성이 높고 그 피해는 생각보다 훨씬 더 클 수 있다.

딥페이크 영상은 악의적인 목적으로 가지고 만들어져 정치적, 사회적으로 대중을 선동하는데 사용될 가능성이 있다. 또한 언론사를 사칭한 가짜뉴스를 만들어서 금융 시장을 교란시킬 수도 있으며, 위성사진, 과학관련 영상이나 데이터 등을 조작하여 외교적 및 군사적 갈등을 일으킬 수도 있다. 또한, 음성 데이터를 이용하여 음성 기반 보안 시스템을 해킹할 수도 있으며, 사람의 손 글씨를 변환하여 중요한 공문서 혹은 사문서를 조작하는데 사용될 수 있다.

딥페이크 기술이 특히 악용될 수 있는 곳은 음란물이다. 현재 딥페이크 기술이 가장 적극적으로 널리 악용되고 있는 분야이기도 하다. 딥페이크는 유명 연예인의 얼굴을 포르노배우의 얼굴과 바꿔치기 함으로써 마치 그들이 포르노그래피 사진이나 영화를 직접 찍은 것처럼 만들어버린다. 중국에서 만들어진 Zao라는 앱(App.)은 사용자가 손쉽게 사람의 얼굴을 바꿔치기할 수 있는 인터페이스를 제공하기도 하였다. 일반인이 손쉽게 소수의 데이터만으로 딥페이크 영상을 제작할 수 있게 되면, 각종 딥페이크 영상의 범람으로 사회적인 부작용이 심각할 것이다.

기술적으로 딥페이크 기술이 발전하는 속도가 워낙 빠르고, 기술의 발전 자체를 막을 수는 없기 때문에 기술적인 측면에서 대책을 내어 놓기는 쉽지 않다. 다만 딥페이크 생성기술의 발전에 맞추어서 딥페이크 감별기술을 꾸준히 발전시키는 것이 대책의 하나가 될 수 있을 것이다.

현재의 기술의 수준으로 딥페이크 기술을 제어할 수 있는 방법으로는, ㉠ 데이터

셋의 크기를 키워서 이를 기반으로 학습된 검출 알고리즘의 성능 향상을 도모하는 것, ㉔ 소셜 미디어(social media) 등에 업로드될 때 선제적으로 검출 알고리즘을 수행하여 데이터를 인증하는 것, ㉕ 발견한 영상의 소스 영상(source image)을 추적할 수 있을 때만 실사임을 가정하고 블록체인을 사용하여 딥페이크를 검출하는 것 등이 있을 수 있다.

위와 같은 방법들이 어느 정도 유효하기는 하지만, 딥페이크는 검출 및 해결하고자 하는 편이 늘 후행할 수밖에 없다. 이 점은 해킹(hacking)과 비슷하다. 악용될 가능성이 긍정적인 면으로 이용될 가능성보다 훨씬 높은 것이다. 딥페이크 기술은 데이터를 조작하고자 하는 사람이 새로운 기술을 개발하여 어느 정도 성과를 거둔 후에야 비로소 검출 문제를 해결하기 위한 여건이 조성된다.

따라서 이러한 딥페이크 기술의 특정상 기술로서만 통제하는 것은 한계가 있으며, 딥페이크 기술을 법적, 제도적으로 규제해야할 필요성이 있다.

5. 소결

위에서 살펴본 바와 같이 딥페이크 생성기술은 이전보다 적은 양의 학습 자료로 원본 영상과의 오차범위를 줄여나가고 있으며, 최종 딥페이크 영상 도출시간을 단축시키고 있다. 딥페이크 기술의 발전으로 단 1장의 사진으로도 딥페이크 영상을 제작할 수 있을 정도로 영상 제작과정이 간소화·간편화되었다.

위와 같은 딥페이크 영상을 감별하기 위한 여러 가지 기술도 등장하고 있다. 구글, 페이스북 등 기업은 딥페이크 영상 감별을 위한 기술 발전을 위해 딥페이크 영상 데이터베이스를 제공하거나 감별대회를 개최하는 등의 노력을 기울이고 있다.

딥페이크 기술의 유용성은 분명히 존재하고 기업은 수익성을 위해 딥페이크 기술을 더욱 발전시켜야 하는 강력한 동기가 있는 반면, 딥페이크 감별 및 식별 기술의 발전 동력은 상대적으로 약한 상황이다. 이러한 현실적인 문제로 딥페이크 기술 개발 속도

를 딥페이크 기술 감별의 속도가 따라잡지 못하고 있다.

이처럼 딥페이크 감별 또는 식별 기술은 기술발전의 동력이 부족하다는 한계가 있는바, 피해보호를 위해 국가적인 차원에서 기술발전을 지원해야 할 필요성이 있다.

제2절 딥페이크 관련 해외 입법 동향

1. 서설

딥페이크에 대한 입법논의가 가장 활발하게 이루어지고 있는 곳은 미국이다. 그 외 EU 및 유럽국가, 호주, 일본, 중국 등에서 딥페이크에 대해 어떻게 입법적으로 대응하고 있는지 살펴본다.

2. 미국

미국은 딥페이크로 인한 법적분쟁을 프라이버시 보호 및 명예훼손, 성매매 알선 사이트 규제 등의 측면에서 접근하였으나, 최근 딥페이크만을 규제하기 위한 독립된 법안이 발의되고 있는 상황이다. 최근 발의되는 법안들은 딥페이크의 규제대상, 예외사항, 형사처벌, 민사배상범위, 플랫폼사업의 책임범위 등에 관하여 상당히 구체적인 내용을 담고 있다.

이하에서는 미국의 딥페이크 관련 입법 동향에 대해 연방법률과 주 법률로 나누어 살펴본다.

2.1. 연방차원의 딥페이크 관련 입법 현황

2.1.1. 통신품위법과 온라인 성매매 퇴치법

통신품위법(47 U.S. Code § 230. Protection for private blocking and screening of

offensive material)은 플랫폼에 게시된 게시물 또는 정보가 문제되는 경우 플랫폼 기업의 책임범위에 관하여 규정하고 있다.

기존에는 플랫폼 기업의 포괄적인 면책을 규정하고 있어 적절한 대치를 면책조건으로 하자는 개정논의가 이루어져 왔다(동법 (c)).

§ 230. Protection for private blocking and screening of offensive material

(c) Protection for “Good Samaritan” blocking and screening of offensive material

(1) Treatment of publisher or speaker

No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider.

(2) Civil liability

No provider or user of an interactive computer service shall be held liable on account of—

(A) any action voluntarily taken in good faith to restrict access to or availability of material that the provider or user considers to be obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable, whether or not such material is constitutionally protected; or

(B) any action taken to enable or make available to information content providers or others the technical means to restrict access to material described in paragraph (1).

이에 2018. 4. 11. 개정을 통하여 (c)(2)(A)³⁹⁾를 제외하고는 성매매법(sex trafficking law)⁴⁰⁾ 적용에 영향이 없도록 하는 규정을 신설하고, 성매매 관련 플랫폼 사업자에게 일정부분 책임을 지울 수 있도록 했다(동조 (e)(5)).

39) (c)(2)(A)는 플랫폼 기업이나 사용자가 음란물 등에 대한 접근 또는 가용성을 제한하기 위해 선의(in good faith)로 자발적으로(voluntarily) 취한 모든 조치에 대하여 민사책임을 지지 않는다는 규정이다.

40) 통신망위법 § 230 (e)(5)의 ‘sex trafficking law’는 온라인 성매매 퇴치법(Allow States and Victims to Fight Online Sex Trafficking Act)를 의미한다.

§ 230. Protection for private blocking and screening of offensive material

(e) Effect on other laws

(1) 내지 (4) 생략

(5) No effect on sex trafficking law

Nothing in this section (other than subsection (c)(2)(A)) shall be construed to impair or limit—

(A) any claim in a civil action brought under section 1595 of title 18, if the conduct underlying the claim constitutes a violation of section 1591 of that title;

(B) any charge in a criminal prosecution brought under State law if the conduct underlying the charge would constitute a violation of section 1591 of title 18; or

(C) any charge in a criminal prosecution brought under State law if the conduct underlying the charge would constitute a violation of section 2421A of title 18, and promotion or facilitation of prostitution is illegal in the jurisdiction where the defendant's promotion or facilitation of prostitution was targeted.

위 통신망위법 § 230가 개정된 2018. 4. 11.과 같은 날 온라인 성매매 퇴치법(Allow States and Victims to Fight Online Sex Trafficking Act)이 발효되었다⁴¹⁾.

온라인 성매매 퇴치법은 온라인 성매매 알선이 이뤄지는 '상호 컴퓨터 서비스(interactive computer service)'의 소유·관리·운영자에 대한 벌금 또는 10년 이하 징역의 처벌을 규정하고 있으며, 플랫폼 사업자가 온라인 성매매 알선이 이루어지는 플랫폼을 제공한 경우 형사처벌의 대상이 된다.

통신망위법 개정 이전에는, 포괄적인 면책조항으로 인하여 온라인 성매매 광고나 홍보물이 게재되는 웹사이트의 관리자에 대해 법적책임을 묻기가 어려웠으나, 통신망위법의 개정 및 온라인 성매매 퇴치법의 시행으로 인하여 웹사이트 관리자, 플랫폼 사업자에게도 온라인 성매매 광고나 홍보물의 게시로 인한 형사책임을 물을 수 있게

41) 이 법은 도널드 트럼프 대통령이 서명하는 즉시 발효되도록 되어있었으며, 2018. 4. 11. 트럼프 대통령이 서명하였다. 이 법은 'Stop Enabling Sex Traffickers Act (SESTA)'와 'Allow States and Victims to Fight Online Sex Trafficking Act (FOSTA)'의 패키지 법안에 해당한다.

되었다(온라인 성매매 퇴치법 SEC. 3. (a),(b)). 피해자는 플랫폼 사업자에게 민사상 손해배상을 청구할 수 있고(온라인 성매매 퇴치법 SEC. 3. (c)), 법원은 배상명령을 할 의무가 있다(온라인 성매매 퇴치법 SEC. 3. (d)).

Allow States and Victims to Fight Online Sex Trafficking Act

SEC. 2. <<NOTE: 47 USC 230 note.>> SENSE OF CONGRESS.

It is the sense of Congress that--

(1) section 230 of the Communications Act of 1934⁴²⁾ (47 U.S.C. 230; commonly known as the ``Communications Decency Act of 1996") was never intended to provide legal protection to websites that unlawfully promote and facilitate prostitution and websites that facilitate traffickers in advertising the sale of unlawful sex acts with sex trafficking victims;

(2) websites that promote and facilitate prostitution have been reckless in allowing the sale of sex trafficking victims and have done nothing to prevent the trafficking of children and victims of force, fraud, and coercion; and

(3) clarification of such section is warranted to ensure that such section does not provide such protection to such websites.

SEC. 3. PROMOTION OF PROSTITUTION AND RECKLESS DISREGARD OF SEX TRAFFICKING.

(a) Promotion of Prostitution.--Chapter 117 of title 18, United States Code, is amended by inserting after section 2421 the following:

``Sec. 2421A. <<NOTE: 18 USC 2421A.>> Promotion or facilitation of prostitution and reckless disregard of sex trafficking

``(a) In General.--Whoever, using a facility or means of interstate or foreign commerce or in or affecting interstate or foreign commerce, owns, manages, or operates an interactive computer service (as such term is defined in defined in section 230(f) the Communications Act of 1934

42) 통신망위법

(47 U.S.C. 230(f))), or conspires or attempts to do so, with the intent to promote or facilitate the prostitution of another person shall be fined under this title, imprisoned for not more than 10 years, or both.

“(b) Aggravated Violation.—Whoever, using a facility or means of interstate or foreign commerce or in or affecting interstate or foreign commerce, owns, manages, or operates an interactive computer service (as such term is defined in defined in section 230(f) the Communications Act of 1934 (47 U.S.C. 230(f))), or conspires or attempts to do so, with the intent to promote or facilitate the prostitution of another person and—

“(1) promotes or facilitates the prostitution of 5 or more persons; or

“(2) acts in reckless disregard of the fact that such conduct contributed to sex trafficking, in violation of 1591(a), shall be fined under this title, imprisoned for not more than 25 years, or both.

“(c) Civil Recovery.—Any person injured by reason of a violation of section 2421A(b) may recover damages and reasonable attorneys' fees in an action before any appropriate United States district court.

“(d) Mandatory Restitution.—Notwithstanding sections 3663 or 3663A and in addition to any other civil or criminal penalties authorized by law, the court shall order restitution for any violation of subsection (b)(2). The scope and nature of such restitution shall be consistent with section 2327(b).

위 통신망위법 및 온라인 성매매 퇴치법에 따라 딥페이크 영상이 온라인 성매매광고나 홍보물로 사용되는 경우 해당 게시물이 올라온 웹사이트 관리자, 플랫폼 사업자에게 책임을 물을 수 있다.

2.1.2. 2018 악성 딥페이크 방지법

2018 악성 딥페이크 방지법(Malicious Deep Fake Prohibition Act of 2018)⁴³⁾은 딥

43) <https://www.congress.gov/bill/115th-congress/senate-bill/3805/text?format=txt>

페이크 규제만을 위하여 발의된 법안으로 의미가 있으나, 2018. 12. 21. 의회 제출된 후 기간 만료로 폐기되었다. 벤 새스(Ben Sasse) 상원의원은 본 법안을 재도입하겠다고 하였으나 아직 이행되지는 않고 있다.

위 법안에서는 딥페이크를 '합리적인 사람들에게 그 기록이 실제로 말한 것이나 행동한 것처럼 보이도록 허위로 만들어지거나 수정된 시청각 기록물'로 정의하였다 (SEC. 2. (a)(2)).

SEC. 2. FRAUD IN CONNECTION WITH AUDIOVISUAL RECORDS.

(a) Definitions.--In this section

(2) the term 'deep fake' means an audiovisual record created or altered in a manner that the record would falsely appear to a reasonable observer to be an authentic record of the actual speech or conduct of an individual

또한 위 법안은 범죄나 불법행위를 유발시킬 목적으로 딥페이크를 만들어내는 행위와 어떤 시청각 기록이 딥페이크임을 알면서 범죄나 불법행위를 유발시킬 목적으로 딥페이크를 유포하는 행위를 금지하고(SEC. 2. (b)), 이를 위반하는 경우에는 벌금형⁴⁴⁾ 또는 2년 이하의 징역형 또는 벌금형과 2년 이하의 징역형의 병과형으로 처벌한다고 규정하고 있다(SEC. 2. (c)(1)). 특히 딥페이크의 생성, 복제, 배포가 행정, 입법, 사법절차 수행 등에 영향을 미치거나 폭력을 조장하는 경우에는 벌금형 또는 10년 이하의 징역형 또는 벌금형과 10년 이하의 징역형의 병과형으로 처벌한다고 규정하고 있다 (SEC. 2. (c)(2)).

44) 본 법안상 구체적인 벌금 액수는 정하고 있지 아니하다. 다만 미국은 18 U.S. Code § 3559.Sentencing classification of offenses, 18 U.S. Code § 3571.Sentence of fine 및 연방형사소송규칙에서 법정형 상한을 기준으로 범죄를 중죄와 경죄로 구분하고 있으며, 여기에 경미범죄 개념을 추가하고 경죄 또는 경미범죄에 대한 여러 간이한 처리절차를 적용하고 있다. 이에 따라서 벌금형의 액수도 달라진다. 본 법안의 경우 벌금형 또는 5년 이하의 징역에 처한다고 정하는 점에서 중죄(felony) 중 classD에 해당하는 것으로 보이고, 이에 따른 벌금형은 25만 달러 이하인 것으로 판단된다.

SEC. 2. FRAUD IN CONNECTION WITH AUDIOVISUAL RECORDS.

(b) Offense.--It shall be unlawful to, using any means or facility of interstate or foreign commerce--

((1) create, with the intent to distribute, a deep fake with the intent that the distribution of the deep fake would facilitate criminal or tortious conduct under Federal, State, local, or Tribal law; or

((2) distribute an audiovisual record with--

((A) actual knowledge that the audiovisual record is a deep fake; and

((B) the intent that the distribution of the audiovisual record would facilitate criminal or tortious conduct under Federal, State, local, or Tribal law.

((c) Penalty.--Any person who violates subsection (b) shall be--

((1) fined under this title, imprisoned for not more than 2 years, or both; or

((2) fined under this title, imprisoned for not more than 10 years, or both, in the case of a violation in which the creation, reproduction, or distribution of the deep fake could be reasonably expected to-- (

((A) affect the conduct of any administrative, legislative, or judicial proceeding of a Federal, State, local, or Tribal government agency, including the administration of an election or the conduct of foreign relations; or

((B) facilitate violence.

한편, 위 법안은 인터넷 서비스 제공자가 선의로 딥페이크에 대한 접근 또는 가용성(availability)을 제한하기 위한 조치를 선의(in good faith)로 자발적(voluntarily)으로 취한 경우((d)(1)(A)), 콘텐츠 제공자 등에게 딥페이크에 대한 접근을 제한하는 기술적 수단을 사용할 수 있게 조치한 경우((d)(1)(B)) 등에는 인터넷 서비스 제공자, 플랫폼 사업자에게 책임을 지지 않도록 하고 있다(SEC. 2. (d)(1)).

SEC. 2. FRAUD IN CONNECTION WITH AUDIOVISUAL RECORDS.

(d) Limitations.--

“(1) In general.--For purposes of this section, a provider of an interactive computer service shall not be held liable on account of--

“(A) any action voluntarily taken in good faith to restrict access to or availability of deep fakes; or

“(B) any action taken to enable or make available to information content providers or other persons the technical means to restrict access to deep fakes.

위 법안은 비록 본격적으로 시행되지는 못하였으나, 딥페이크에 대해서 정의한 점, 딥페이크 생성 및 유포에 대해 형사처벌규정을 둔 점, 인터넷 사업자의 책임 범위에 관하여 규정한 점에서 의의가 있다.

2.1.3. 2019년 딥페이크 보고법 (Deepfakes Report Act of 2019)

2019년 딥페이크 보고법(Deepfakes Report Act of 2019)은 2019. 7. 9. 법안이 제출되어, 2019. 10. 24. 상원을 통과하여 2019. 10. 28. 하원에 회부되었으며, 이후 에너지 통상위원회(the House Committee on Energy and Commerce)에 회부되었고, 2019. 10. 29. 소비자 보호 및 상거래 소위원회(the Subcommittee on Consumer Protection and Commerce)에 회부된 상태이다.

위 법안은 딥페이크에 대한 정의를 따로 두지 아니하고, '디지털 콘텐츠 위조(digital content forgery)'에 대한 정의 규정을 두고 있다. 위 법안은 인공지능 및 기계 학습 기술을 포함한 신기술을 사용하여 (실제라고) 오해를 일으키기 위해 청각적, 시각적, 문자적 콘텐츠를 제작 또는 조작하는 것을 디지털 콘텐츠 위조라고 정의하였다. 또한 관련 장관을 국토안보부 장관으로 설정하였다(SEC. 2).

SEC. 2. DEFINITIONS.

In this Act:

(1) DIGITAL CONTENT FORGERY.—The term “digital content forgery” means the use of emerging technologies, including artificial intelligence and machine learning techniques, to fabricate or manipulate audio, visual, or text content with the intent to mislead.

(2) SECRETARY.—The term “Secretary” means the Secretary of Homeland Security.

위 법안은 발효 후 1년 이내, 이후 매년 5년 동안 딥페이크 기술의 상태와 활용현황을 평가하는 심층조사와 보고서발표, 공정회 개최할 것을 주요내용으로 하고 있다 (SEC. 3 (a),(c)). 국토안보부 과학기술본부 차관(Under Secretary for Science and Technology)을 거쳐 국토안보부 장관(Secretary of Homeland Security)이 보고서 작성 주체가 된다⁴⁵⁾.

SEC. 3. REPORTS ON DIGITAL CONTENT FORGERY TECHNOLOGY.

(a) In General.—Not later than 1 year after the date of enactment of this Act, and annually thereafter for 5 years, the Secretary, acting through the Under Secretary for Science and Technology, shall produce a report on the state of digital content forgery technology.

(c) Consultation And Public Hearings.—In producing each report required under subsection (a), the Secretary may—

(1) consult with any other agency of the Federal Government that the Secretary considers necessary; and

(2) conduct public hearings to gather, or otherwise allow interested parties an opportunity to present, information and advice relevant to the production of the report.

45) 국토안보부 내 과학기술본부의 차관(Under Secretary)을 거쳐 국토안보부 장관이 보고서를 작성하는 것으로 되어있다. 미국 국토안보부 과학기술본부는 국토안보부를 포함해 미국 내 여러 기관이 필요로 하는 국민안전·재난재해 대응과 관련한 기술을 개발·지원하는 차관급 조직이다.

위 법안에 따라 작성되는 보고서는 ① 디지털 콘텐츠 위조의 제작 또는 전파에 사용되는 기술(진화 포함)의 평가, ② 디지털 콘텐츠 위조 유형에 대한 설명, ③ 외국정부가 국가 안보에 해를 끼치기 위하여 디지털 콘텐츠를 위조하여 사용하는 방법에 대한 평가, ④ 미국 정부기관 이외에 기관 또는 단체에서 디지털 콘텐츠 위조를 사용하는 방법에 대한 평가, ⑤ 고도의 인공 콘텐츠를 만들어내는 딥러닝 기술에 대한 평가, ⑥ 디지털 콘텐츠가 위조되었음을 판별할 수 있는 방법에 대한 분석 및 위조된 것으로 의심되는 콘텐츠를 식별하기 위한 방법에 대한 권장사항, 콘텐츠 사용자에게 대한 경고의 제공 등, ⑦ 디지털 콘텐츠 위조 기술을 해결하기 위한 기술적 대책에 대한 설명, ⑧ 그 밖에 장관이 적절하다고 판단하는 내용을 담고 있어야 한다(SEC. 3 (b)).

SEC. 3. REPORTS ON DIGITAL CONTENT FORGERY TECHNOLOGY.

(b) Contents.—~~Each report produced under subsection (a) shall include—~~

- (1) an assessment of the underlying technologies used to create or propagate digital content forgeries, including the evolution of such technologies;
- (2) a description of the types of digital content forgeries, including those used to commit fraud, cause harm, or violate civil rights recognized under Federal law;
- (3) an assessment of how foreign governments, and the proxies and networks thereof, use, or could use, digital content forgeries to harm national security;
- (4) an assessment of how non-governmental entities in the United States use, or could use, digital content forgeries;
- (5) an assessment of the uses, applications, dangers, and benefits of deep learning technologies used to generate high fidelity artificial content of events that did not occur, including the impact on individuals;
- (6) an analysis of the methods used to determine whether content is genuinely created by a human or through digital content forgery technology and an assessment of any effective heuristics used to make such a determination, as well as recommendations on how to identify and address suspect content and elements to provide warnings to users of the content;
- (7) a description of the technological counter-measures that are, or could be, used to address concerns with digital content forgery technology; and
- (8) any additional information the Secretary determines appropriate.

위 법안은 딥페이크 관련 현황을 보고서로 작성하도록 하고, 보고서에 담길 내용을 구체화하였으며, 공청회를 개최하도록 규정한 것에 의의가 있다.

2.1.4. 2019년 책임법에 따라 부당한 이용으로부터 유래한 허위의 외관으로부터 모든 사람들을 보호하기 위한 법률

이벳 클락(Yvette Clarke) 하원의원은 2019. 6. 12. 2019년 '책임법에 따라 부당한 이용으로부터 유래한 허위의 외관으로부터 모든 사람들을 보호하기 위한 법률 (Defending Each and Every Person from False Appearances by Keeping Exploitation Subject to Accountability Act of 2019)'이라는 법안을 발의하였다. 해당 법안은 2019. 6. 13. 에너지통상위원회(Committee on Energy and Commerce), 2019. 6. 24. 국토안보위원회(Committee on Homeland Security), 2019. 6. 28. 법사위원회(Committee on the Judiciary)에 각 회부되어 있는 상황이다.

위 법안은 딥페이크를 '(A) 실제로 그러한 언행에 관여하지 않은 사람의 말이나 행동을 사실적으로 묘사하는 것으로 보이는 것 또는 (B) 다른 사람의 신체적 언어적 능력보다는 기술적 수단에 실질적으로 의존한 것에 관한 영상 녹화, 영화용 필름, 음성 녹음, 전자 이미지 또는 사진, 언어의 기술적 표현 또는 실질적으로 파생된 행위라고 정의하고 있다(SEC. 2 (n)(3)).

SEC. 2. TRANSPARENCY REQUIREMENTS.

“§ 1041. Advanced technological false personation record

(n) Definitions.

(3) DEEP FAKE.—The term ‘deep fake’ means any video recording, motion-picture film, sound recording, electronic image, or photograph, or any technological representation of speech or conduct substantially derivative thereof—

“(A) which appears to authentically depict any speech or conduct of a person who did not in fact engage in such speech or conduct; and

“(B) the production of which was substantially dependent upon technical means, rather than the ability of another person to physically or verbally impersonate such person.

위 법안은 주간(interstate) 또는 외국과의 상거래 수단이나 시설을 이용하여, 인터넷을 통해 배포하려는 의도로 첨단 기술 허위 개인화 기록(an advanced technological false personation record)을 생산하거나 그 기록이 배포되어야 하는 지식을 생산하는 자는, (b)항에 따른 워터마크 요구 사항, 시청각기록의 경우 (c)항에 따른 공개요건, 영상기록의 경우 (d)항에 따른 공개요건, 오디오 레코드의 경우 (e)항에 따른 공개요건을 준수하여야 한다고 정하고 있다(SEC. 2 (a)).

한편, 위 법안은 (A) (c)항, (d)항, (e)항의 방법보다 합리적인 사람이라면 더욱 명확하게 허위임을 알 수 있는 방법을 사용한 경우, (B) 궁극적으로 배포된 기록이 합법적인 경우(in compliance), (C) 공연예술가 등 실존 인물의 영상이나 음반을 주로 수록하고 있으며, 실질적으로 디지털로 수정되지 않은 경우, (D) 영화, 텔레비전, 음악 또는 이와 유사한 제작물을 편집하거나 그 제작물을 파생적으로 제작하는 것과 관련하여, 출연자가 원래 출연자의 출연에 동의하는 이 법의 제정 이전에 만들어진 원본 내용인 경우, (E) 패러디 쇼나 출판물, 역사적 재현, 허구화된 라디오, 텔레비전, 영화 프로그래밍 등 합리적인 사람이라면 오인하지 않는 사안인 경우, (F) 미국의 장교나 직원이 생산하거나 그 권한에 따라 공공 안전이나 국가 안보를 증진시키기 위해 생산된 첨단 기술 허위 개인화 기록(an advanced technological false personation record)의 경우에는 예외로 하여 법안을 적용하지 않고 있다(SEC. 2 (j)(1)). 그리고 (b)의 워터마크 요건은 법무부장관(the Attorney General)이 규정으로 결정한 첨단 기술 허위인격기록의 등급에 대해서는 적용되지 않는다(SEC. 2 (j)(2)).

SEC. 2. TRANSPARENCY REQUIREMENTS.

“§ 1041. Advanced technological false personation record

“(a) In General.—~~Except as provided in subsection (j), any person who, using any m~~

means or facility of interstate or foreign commerce, produces an advanced technological false personation record with the intent to distribute such record over the internet or knowledge that such record shall be so distributed, shall ensure such record, complies with—

“(1) the watermark requirement under subsection (b); and

“(2) (A) in the case of an audiovisual record, the disclosure requirements under subsection (c);

“(j) Exceptions.—

“(1) DISCLOSURE.—The requirements under subsections (c), (d), and (e) shall not apply with respect to any advanced technological false personation record—

“(A) containing alternative disclosures regarding the falsity of the exhibited material activities which a reasonable person would deem to be more prominent than those required under subsection (c), (d), or (e), as the case may be;

“(B) during the process of producing such record, provided the ultimately distributed record is in compliance;

“(C) which primarily contains images or sound recordings of actual persons, such as performing artists, and have not been substantially digitally modified;

“(D) created in connection with editing a motion picture, television, music, or similar production or creating a derivative production thereof, the original content of which was created prior to the enactment of this Act, in which the person appearing provided consent to their original appearance;

“(E) appearing in a context such that a reasonable person would not mistake the falsified material activity for actual material activity of the exhibited living person, such as parody shows or publications, historical reenactments, or fictionalized radio, television, or motion picture programming; or

“(F) produced by an officer or employee of the United States, or under the authority thereof, in furtherance of public safety or national security.

“(2) WATERMARK.—The watermark requirement under subsection (b) shall not apply with respect to any class of advanced technological false personation records which the Attorney General determines by regulation should be excluded from such requirement.

위 법안이 적용되는 경우 움직이는 시각적 요소를 포함하는 첨단 기술 허위 개인화 기록(an advanced technological false personation record)에는 변경된 오디오 또는 시각적 요소를 식별할 수 있도록 내장형 디지털 워터마크를 포함하여야 한다.(SEC. 2

(b)),

시각적 요소만을 포함하는 첨단 기술 허위 개인화 기록(an advanced technological false personation record)의 경우에는, 시각적 요소가 지속되는 기간 동안 변경된 시각적 요소와 변경의 범위에 관한 간결한 설명이 나타나도록 영상 하단에 명확하게 표시하여야 한다(SEC. 2 (d)).

청각적 요소만을 포함하는 첨단 기술 허위 개인화 기록(an advanced technological false personation record)의 경우에는, 해당 기록이 포함하고 있는 변경된 청각적 요소와 변경의 범위에 관한 간결한 설명에 관하여, 해당 기록의 시작 부분에서 명확하게 구두 설명을 하여야 한다(SEC. 2 (e)).

SEC. 2. TRANSPARENCY REQUIREMENTS.

“§ 1041. Advanced technological false personation record

“(b) Digital Watermark.—Any advanced technological false personation record which contains a moving visual element shall contain an embedded digital watermark clearly identifying such record as containing altered audio or visual elements.

“(d) Visual Disclosure.—Any advanced technological false personation records exclusively containing a visual element shall include an unobscured written statement in clearly readable text appearing at the bottom of the image throughout the duration of the visual element that identifies the record as containing altered visual elements, and a concise description of the extent of such alteration.

“(e) Audio Disclosure.—Any advanced technological false personation records exclusively containing an audio element shall include, at the beginning of such record, a clearly articulated verbal statement that identifies the record as containing altered audio elements and a concise description of the extent of such alteration, and in the event such record exceeds two minutes in length, not less than 1 additional clearly articulated verbal statement and additional concise description at some interval during each two-minute period thereafter.

위 법안은 SEC. 2 (a)를 고의로 위반한 자로서 ① 거짓으로 등장하는 사람을 모욕하거나 다른 방법으로 괴롭히려는 의도를 가지고 첨단 기술 허위 개인화 기록(an advanced technological false personation record)에 성적인 내용이 포함되어 있고 성

행위를 하거나 나체 상태에 있는 사람이 등장하도록 한 경우, ② 첨단 기술 허위 개인화 기록(an advanced technological false personation record)이 폭력이나 신체적 위협, 무장 또는 외교적 충돌 유발, 선거 등 공식적 절차 방해 등을 선동하거나 진전시킬 가능성이 있는 신뢰 가능한 위협이 되는 경우, ③ 증권 사기, 유선 사기, 사칭, 또는 신분 도용 등 사기와 관련한 범죄행위를 하는 경우, ④ 국내 공공 정책 토론에 영향을 미치거나 연방, 주, 지방 또는 영토 선거에 개입하거나 그러한 권력이 합법적으로 수행할 수 없는 기타 행위에 관여할 목적을 가진 외국 권력자 또는 그 대리인의 경우에는 벌금⁴⁶⁾ 또는 5년 이하의 징역에 처한다(SEC. 2 (f)(1)(A)).

그리고 누구든지 첨단 기술 허위 개인화 기록(an advanced technological false personation record)을 배포하려는 의도로 (a)항에 따라 요구되는 워터마크를 제거하거나 공개 요건을 모호하게 만드는 경우 벌금⁴⁷⁾ 또는 5년 이하의 징역에 처하도록 하였다(SEC. 2 (f)(1)(B)).

SEC. 2. TRANSPARENCY REQUIREMENTS.

“§ 1041. Advanced technological false personation record

(f) Penalty.—

“(1) CRIMINAL PENALTY.—

“(A) FAILURE TO DISCLOSE.—Whoever knowingly violates subsection (a)—

“(i) with the intent to humiliate or otherwise harass the person falsely exhibited, provided the advanced technological false personation record contains sexual content of a visual nature and appears to feature such person engaging in such sexual acts or in a state of nudity;

46) 본 법안상 구체적인 벌금 액수는 정하고 있지 아니하다. 다만 미국은 18 U.S. Code § 3559.Sentencing classification of offenses, 18 U.S. Code § 3571.Sentence of fine 및 연방형사소송규칙에서 법정형 상한을 기준으로 범죄를 중죄와 경죄로 구분하고 있으며, 여기에 경미범죄 개념을 추가하고 경죄 또는 경미범죄에 대한 여러 간이한 처리절차를 적용하고 있다. 이에 따라서 벌금형의 액수도 달라진다. 본 법안의 경우 벌금형 또는 5년 이하의 징역에 처한다고 정하는 점에서 중죄(felony) 중 classD에 해당하는 것으로 보이고, 이에 따른 벌금형은 25만 달러 이하인 것으로 판단된다.

47) 상동

“(ii) with the intent to cause violence or physical harm, incite armed or diplomatic conflict, or interfere in an official proceeding, including an election, provided the advanced technological false personation record did in fact pose a credible threat of instigating or advancing such;

“(iii) in the course of criminal conduct related to fraud, including securities fraud and wire fraud, false personation, or identity theft; or

“(iv) by a foreign power, or an agent thereof, with the intent of influencing a domestic public policy debate, interfering in a Federal, State, local, or territorial election, or engaging in other acts which such power may not lawfully undertake;

shall be fined under this title, imprisoned for not more than 5 years, or both.

“(B) ALTERING DISCLOSURES.—Whoever knowingly alters an advanced technological false personation record to remove or meaningfully obscure the disclosures required under subsection (a) with the intent to distribute such altered record and—

(이하 생략)

위 법안은 (a)항을 위반한 사람은 기록 또는 변경 당 최대 15만 달러의 민사상 벌금과 적절한 금지명령을 받아야 한다고 정하고 있다. 그리고 첨단 기술 허위 개인화 기록(an advanced technological false personation record)을 배포하려는 의도로 (a)항에 따라 요구되는 워터마크를 제거하거나 공개 요건을 모호하게 만드는 경우 최대 15만 달러의 민사상 벌금과 적절한 금지명령을 받아야 한다고 정하고 있다(SEC. 2(f)(2)).

SEC. 2. TRANSPARENCY REQUIREMENTS.

“§ 1041. Advanced technological false personation record

(f) Penalty.—

(2) CIVIL PENALTY.—

“(A) FAILURE TO DISCLOSE.—Any person who violates subsection (a) shall be subject to a civil penalty of up to \$150,000 per record or alteration, as well as appropriate injunctive relief.

“(B) ALTERING DISCLOSURES.—Any person who alters an advanced technological false personation record to remove or meaningfully obscure the disclosures required under subsection (a) with the intent to distribute such altered record shall be subject to a civil penalty of up to \$150,000 per record or alteration, as well as appropriate i

njunctive relief.

위 법안은 피해자가 범위반자에 대하여 손해배상청구를 하는 것에 관하여도 규정하고 있다(SEC. 2 (g)). 위 법안은 독특하게 사안에 따라 차등하여 손해배상청구 금액을 정하고 있다. (g))(2)에서는 손해배상금액에 관하여, (A) 피해자가 실제로 입은 손해와 (a)항을 위반하여 워터마크를 제거하거나 공개 요건을 모호하게 만든 자가 실질적으로 얻은 파생 이익으로 인한 추가적인 손해, (B) 피해자가 인지할 수 있는 피해를 입었거나 그러한 피해를 경험할 수 있는 가시적 위험에 직면한 경우 기록당 5만 달러, (C) 기록이 피해자에 의한 극단적이거나 터무니없는 행위를 묘사하는 것으로 간주되어 피해자가 인지할 수 있는 피해를 입었거나 그러한 피해를 경험할 수 있는 가시적 위험에 직면한 경우 기록당 10만 달러, (D) 첨단 기술 허위 개인화 기록(an advanced technological false personation record)에 성행위를 하거나 나체 상태에 있는 것으로 잘못 묘사되어 피해자를 모욕하거나 괴롭히기 위한 시각적 성격의 노골적 성적 내용이 포함된 경우 기록 당 15만 달러 중 더 큰 것으로 한다고 정하여, 경우에 따라 손해배상금액을 차등하여 규정하고 있다.

SEC. 2. TRANSPARENCY REQUIREMENTS

“§ 1041. Advanced technological false personation record

“(g) Private Right Of Action.—

“(1) IN GENERAL.—Any living individual or affiliated corporate or other entity who has been exhibited as engaging in falsified material activity in an advanced technological false personation record may bring a civil action before the appropriate Federal district court for damages under paragraph (2) and injunctive relief under paragraph (3) against a person who violates subsection (a) or alters an advanced technological false personation record to remove or meaningfully obscure the disclosures required under subsection (a).

“(2) DAMAGES.—Damages shall consist of the greater of—

“(A) actual damages suffered by the living person or the affiliated corporation or entity, and any additional substantially derivative profits of the person who violated su

bsection (a) or altered an advanced technological false personation record to remove or meaningfully obscure the disclosures required under subsection (a);

“(B) \$50,000 per record, if the living person or affiliated corporation or entity experienced a perceptible individual harm or faced a tangible risk of experiencing such;

“(C) \$100,000 per record, if the living person or affiliated corporation or entity experienced a perceptible individual harm or faced a tangible risk of experiencing such and the record purported to depict extreme or outrageous conduct by the living person; or

“(D) \$150,000 per record, if the advanced technological false personation record contains explicit sexual content of a visual nature intended to humiliate or otherwise harass the person falsely depicted as engaging in such sexual acts or in a state of nudity.

위 법안은 법무부장관으로 하여금 시청각 콘텐츠 제작자가 본 법안에 따라 제안된 제작물의 적법성에 관한 자문 의견을 구할 수 있도록 하는 절차를 확립해야 할 의무를 규정하고(SEC. 2 (k), (1), (A)), 본 법안의 제정일로부터 1년 이내에 디지털 워터마크의 기술 사양에 관한 규칙을 발표할 의무도 규정하고 있다(SEC. 2 (k),(3)).

또한 위 법안은 법무부장관으로 하여금, 다른 관련 연방기관과 협력하여, 본 법안의 제정일로부터 5년 후 및 그로부터 5년 후에 국회에 보고서를 제출할 의무를 규정하는데, 이때 보고서는 본 법안에서 추구된 형사처벌 및 민사상 벌금과 관련된 경향을 설명하고, 새로운 기술의 출현에 의하여 필요하게 된 본 법안의 업데이트를 권고하도록 규정한다(SEC. 2 (o)).

SEC. 2. TRANSPARENCY REQUIREMENTS

“§ 1041. Advanced technological false personation record

“(k) Advisory Opinions, Waiver, And Standards.—

“(1) ADVISORY OPINIONS.—The Attorney General shall—

“(A) establish a process by which any producer of audio, visual, or audiovisual content may seek an advisory opinion regarding the legality of their proposed production under this section;

(3) WATERMARK STANDARDS.—Not later than 1 year after the date of enactment o

f this section, the Attorney General shall issue rules governing the technical specifications of the digital watermarks required under subsection (b) which shall include, if such is determined appropriate, a requirement for such watermarks to contain embedded metadata.

“(o) Reports.—The Attorney General, in coordination with other relevant Federal agencies, shall submit a report to Congress 5 years after the date of enactment of this section, and 5 years thereafter, describing trends related to prosecutions and civil penalties pursued under this section, and recommending any updates to this section necessitated by the emergence of new technologies.

위 법안은 국토안보부 장관에게 다른 관련 연방기관의 수장과 협력하여, 과학기술국(Science and Technology Directorate) 내에 일명 'Deep Fakes Task Force'를 설립하도록 의무를 부여하는데(SEC. 7 (a)), 'Deep Fakes Task Force'는 ① 딥페이크의 국가 안보 영향에 맞서기 위한 미국 정부의 노력을 위한 것이고((1)), ② 딥페이크 등 발전된 이미지 조작 방법을 감지, 방지, 딥페이크 등 위조된 것과 합법적인 시청각 자료들을 구별하기 위한 기술을 연구·개발하기 위한 것이며((2)), ③ 그러한 기술을 연구하는 다른 연방기관에 행정적, 과학적 지원을 제공하기 위한 것이고((3)), ④ 그러한 기술을 채택하려는 미국 정부의 노력을 장려하기 위한 것이다((4)). 'Deep Fakes Task Force'는 ⑤ 미국 정부와 관련 민간 부문 기업 또는 학계 및 연구기관을 포함한 기타 비정부 기관 사이의 딥페이크 등 발전된 이미지 조작 방법의 식별에 관한 토론 및 적절한 협력을 촉진하기도 한다((5)).

또한 위 법안은 국토안보부 장관에게 본 법안의 제정일로부터 1년 이내에 그리고 그 후 매년 5년 동안 'Deep Fakes Task Force'의 활동, 딥페이크와 관련된 기술적 진보 등에 관한 보고서를 하원의 국토안보위원회(the Committee on Homeland Security)와 상원의 국토안보위원회 및 정부위원회(the Committee on Homeland Security and Governmental Affairs)에 제출할 의무도 부여한다(SEC. 7 (c)).

위 법안은 국토안보부 장관에게 최소한 매년, 하원의 국토안보위원회(the Committee on Homeland Security)와 상원의 국토안보위원회 및 정부위원회(the

Committee on Homeland Security and Governmental Affairs)에 기밀 서면 통지를 해야 할 의무를 부여하고, 요청이 있는 경우, 선거를 포함하여 미국 내 공식 절차에 영향을 미치거나 간섭하기 위하여 딥페이크 기술을 사용하려는 외국의 알려진 시도에 관한 브리핑을 제공해야 할 의무를 부여한다(SEC. 8).

SEC. 8. CONGRESSIONAL NOTIFICATION.

The Secretary of Homeland Security, on no less than an annual basis, shall provide the Committee on Homeland Security of the House of Representatives and the Committee on Homeland Security and Governmental Affairs of the Senate with a classified written notification and, upon request, a briefing regarding any known attempts of foreign states to use deep fake technology to influence or otherwise interfere in an official proceeding within the United States, including an election.

위 법안은 미국 정부가 딥페이크를 확실하게 감지하고, 딥페이크와 합법적인 시청각 자료 및 실제 사건의 시각적 묘사를 구별할 수 있는 기술을 개발하는 경우, 대통령이 미국의 국가 이익에 위배된다고 판단하지 않는 한, 이러한 기술을 미국 민간 부문 인터넷 플랫폼에서도 사용할 수 있도록 하여, 민간 부문과의 협력을 규정한다(SEC. 7 (b)).

SEC. 7. DETECTION OF DEEP FAKES.

(a) Establishment Of Task Force.—The Secretary of Homeland Security, in coordination with the heads of other relevant Federal elements, shall establish a task force within the Science and Technology Directorate, hereinafter referred to as the Deep Fakes Task Force, to—

- (1) advance efforts of the United States Government to combat the national security implications of deep fakes;
- (2) as appropriate, research and develop technologies to detect, or otherwise counter and combat, deep fakes and other advanced image manipulation methods and distinguish such deep fakes or related forgeries from legitimate audiovisual recordings or visual depictions of actual events;

(3) provide support, both administrative and scientific, to other Federal elements researching such technologies;

(4) encourage efforts of the United States Government to adopt such technology; and

(5) facilitate discussion and appropriate cooperation between the United States Government and relevant private sector technology enterprises or other nongovernmental entities, including academic and research institutions, regarding the identification of deep fakes or other advanced image manipulation methods.

(b) Private Sector Collaboration.—In the event the United States Government develops technology to reliably detect deep fakes and distinguish such from legitimate audio visual recordings or visual depictions of actual events, the President shall, unless he determines such is contrary to the national interests of the United States, endeavor to make such technology available to appropriate United States private sector internet platforms, including social networks.

(c) Annual Report.—Not later than one year after the date of the enactment of this Act and annually thereafter for a period of five years, the Secretary of Homeland Security shall submit an unclassified report, which may however contain a classified annex, to the Committee on Homeland Security of the House of Representatives and the Committee on Homeland Security and Governmental Affairs of the Senate describing—

(1) the activities of the Task Force;

(2) as appropriate, technological progress related to the detection of deep fakes;

(3) new developments related to the national security threat posed by deep fakes or related image manipulation technologies, which shall include a description of any efforts of the Russian Federation and the People's Republic of China, and such other states or groups as the Attorney General determines appropriate, to distribute unlawful deep fakes in the United States or other democracies; and

(4) related efforts of the United States to combat and counter deep fakes or related image manipulation technologies.

(d) Definition.—The term “deep fake” shall have the meaning given such term in section 1041 of title 18, United States Code, as added by section 2 of this Act.

2.2. 각 주 별 딥페이크 관련 입법 현황

2.2.1. 뉴욕주

2.2.2.1. 프라이버시권 및 퍼블리시티권에 관한 민권법을 개정하고, 퍼블리시티권 침해 조치 개시의 적시성에 관한 민사관행법 및 규칙을 개정하는 법안

프라이버시권 및 퍼블리시티권에 관한 민권법을 개정하고, 퍼블리시티권 침해 조치 개시의 적시성에 관한 민사관행법 및 규칙을 개정하는 법안(An act to amend the civil rights law, in relation to the right of privacy and the right of publicity; and to amend the civil practice law and rules, in relation to the timeliness of commencement of an action for violation of the right of publicity)은 프라이버시권 및 퍼블리시티권에 관한 민권법을 개정하고, 퍼블리시티권 침해에 대한 조치 개시의 적시성에 관한 민사관행법 및 하위규칙을 개정하는 내용을 담고 있다⁴⁸⁾. 위 법은 2018. 5. 31. 뉴욕주 의회에 제출되고, 2018. 6. 18. 통과되어 현재 시행되고 있다.

위 법은 목적 부분에서 디지털 아바타를 만드는 기술을 다루며 그 기술의 사용에 관한 규제를 하기 위함을 밝히고 있다⁴⁹⁾. 님페이크 영상 속 진짜처럼 보이는 가짜가 바로 디지털 아바타라고 볼 수 있다.

PURPOSE OF BILL

To create a right of publicity for deceased individuals and a registry to publicly post such interests upon thereby giving notice to people who may seek to use an individual's right of publicity in New York State for advertising purposes, or for the purpose of trade. In addition this bill addresses the ability of technology to create **digital avatars** and makes regulations regarding their use.

위 법은 'Digital replica(디지털 복제본)'을 '표사되고 있는 개인의 화상이나 음성을

48) https://nyassembly.gov/leg/?default_fld=&leg_video=&bn=A08155&term=2017&Text=Y

49) https://nyassembly.gov/leg/?default_fld=&leg_video=&bn=A08155&term=2017&Summary=Y

사실적으로 묘사하는 살아있는 또는 사망한 개인의 화상 또는 음성의 컴퓨터 생성 또는 전자적 재생산'이라고 정의하였다(§ 50의 2.)

§ 50. Definitions.

For the purposes of sections fifty-f, fifty-g, fifty-h, fifty-i and fifty-one of this article, the following terms shall have the following meanings:

2. "Digital replica" means a computer-generated or electronic reproduction of a living or deceased individual's likeness or voice that realistically depicts the likeness or voice of the individual being portrayed. A digital replica is included within an individual's portrait.

위 법은 시청각 저작물 등 표현 작업에서 거래 목적으로 Digital replica를 사용하는 경우 위반으로 간주한다(§ 51의 3.). 위 법은 패러디, 풍자, 논평, 비평, 정치적·공익적 목적, 뉴스로서 가치가 있는 정보 등에 Digital replica가 사용된 경우에는 법위반으로 간주하지 않는 예외규정을 두고 있다(§ 51의 3 (b)).

§ 51. Action for injunction and for damages.

3. Digital replica for purposes of trade in an expressive work.

(a) Use of a digital replica, as defined in subdivision two of section fifty of this article, of an individual shall constitute a violation if done without the consent of the individual if the use is:

(i) in a scripted audiovisual or audio work, or in a live performance of a dramatic work, in a manner that is intended to create, and that does create, the clear impression that the individual represented by the digital replica is performing, the activity for which he or she is known, in the role of a fictional character; or

(ii) in a performance of a musical work, in a manner that is intended to create, and that does create, the clear impression that the individual represented by the digital replica is performing, the activity for which he or she is known, in such musical work; or

(iii) in an audiovisual work, in a manner that is intended to create, and that does create, the clear impression that the athlete represented by the digital replica is engaging in an athletic activity for which he or she is known.

(b) Consent for the use of the digital replica of an individual as provided in the provisions of this article shall not be required if such use is:

- (i) for purposes of parody, satire, commentary, or criticism;
- (ii) in a work of political, public interest, or newsworthy value, or similar work, including a documentary, regardless of the degree of fictionalization in the work; or
- (iii) de minimis or incidental.

위 법은 개인의 동의 없이, 그 개인이 수행하고 있다는 인상을 주는 방식으로 음란물에 Digital replica를 사용하는 경우 법 위반으로 간주한다(§ 51의 4.).

§ 51. Action for injunction and for damages.

4. Digital replica use in a pornographic work.

Use of a digital replica of an individual shall constitute a violation if done without the consent of the individual if the use is in an audiovisual pornographic work in a manner that is intended to create and that does create the impression that the individual represented by the digital replica is performing. Nothing in this section shall limit any other rights the individual may have against any party relating to such pornographic work.

위 법 위반으로 인하여 피해를 입은 경우 피해자는 법 위반자에 대하여 손해배상을 청구할 수 있다(§ 51의 6.)

§ 51. Action for injunction and for damages.

6. Action for injunction and for damages.

Any person whose persona is used within this state for advertising purposes, for the purposes of trade without the written consent first obtained as provided in the provisions of this article is entitled to maintain an equitable action in the supreme court of this state against the person so using his or her persona, to prevent and restrain the use thereof; and may also sue and recover damages for any injuries sustained including an amount equal to the greater of seven hundred fifty dollars or compensatory damages by reason of such use and if the defendant shall have knowingly used such person's persona in such manner as is forbidden or declared to be unlawful by the provisions of this article relating to the right of privacy or the right of publicity,

the finder of fact, in its discretion, may award exemplary damages. A violation of an individual's right of privacy or right of publicity may occur without regard to whether the use or activity is for profit or not-for-profit.

위 법은 딥페이크로 생성되는 디지털 복제물에 관하여 정의한 점, 딥페이크를 프라이버시권 및 퍼블리시티권의 관점에서 접근한 점에서 의의가 있다.

2.2.2.2. 퍼블리시티권을 확립하고 성적으로 명백한 묘사를 불법적으로 유포하거나 출판하기 위하여 사적 권리를 제공하는 것과 관련한 민권법 개정법

퍼블리시티권을 확립하고 성적으로 명백한 묘사를 불법적으로 유포하거나 출판하기 위하여 사적 권리를 제공하는 것과 관련한 민권법 개정법(An act to amend the civil rights law, in relation to establishing the right of publicity and to providing a private right of action for unlawful dissemination or publication of a sexually explicit depiction of an individual)은 퍼블리시티권을 확립하고 개인의 성적으로 명백한 묘사를 불법적으로 유포하거나 출판하기 위한 사적 권리를 제공하는 것과 관련한 민권법 개정의 내용을 담고 있다⁵⁰⁾. 위 법은 2019. 5. 16. 법안이 회부되었고, 2020. 7. 22. 상원을 통과하였으며, 2020. 7. 23. 하원을 통과하였다. 또한 2020. 11. 30. 최종 가결되었다.

위 법은 'digital replica(디지털 복제본)'를 '개인에 의하여 새로이 생성되고, 독창적이며, 컴퓨터로 만들어진 전자 수행물이고, 개인이 실제로 수행하지 않은 새로이 생성되고 독창적인 녹음 또는 시청각 작업물인데, 그것이 매우 현실적이어서 합리적인 관찰자는 묘사된 개인에 의한 수행물이며 다른 개인은 아니라고 믿을만한 것'이라고 정의한다(§ 50-f. 1. c.).

위 법은 개인의 독창적이거나 녹음된 연주로 구성된 음원 또는 시청각 작업물의 전

50) https://nyassembly.gov/leg/?default_fld=&leg_video=&bn=S05959&term=2019&Text=Y

자적 복제, 컴퓨터 생성 또는 기타 디지털 리마스터링뿐만 아니라, 다른 소리의 독립적인 고정으로 구성된 녹음의 복제는 그러한 소리가 개인의 목소리를 모방하거나 가창하더라도 digital replica(디지털 복제본)에 포함되지 않는다고 본다(§ 50-f. c.).

Section 1. The civil rights law is amended by adding a new section 50-f to read as follows:

§ 50-f. Right of publicity. 1. For purposes of this section:

(...)

c. "digital replica" means a newly created, original, computer-generated, electronic performance by an individual in a separate and newly created, original expressive sound recording or audiovisual work in which the individual did not actually perform, that is so realistic that a reasonable observer would believe it is a performance by the individual being portrayed and no other individual. A digital replica does not include the electronic reproduction, computer generated or other digital remastering of an expressive sound recording or audiovisual work consisting of an individual's original or recorded performance, nor the making or duplication of another recording that consists entirely of the independent fixation of other sounds, even if such sounds imitate or simulate the voice of the individual.

위 법은 시청각 작품에서 허구의 캐릭터로 또는 음악 작품의 라이브 공연을 위해 사망한 공연자의 digital replica(디지털 복제본)를 사전 동의 없이 사용하는 자는, 그 사용이 대중을 속일 가능성이 있는 경우, 그 손해에 대한 책임을 진다고 규정한다(§ 50-f. 2. b.). 또한 위 법은 사망한 공연자의 digital replica(디지털 복제본) 또는 사망한 공연자의 성명, 음성, 서명, 사진 등을 무단으로 사용하는 것에 대하여 사전에 알고 있었던 것이 아니라면, 신문, 잡지, 라디오, 텔레비전 네트워크, 방송국, 케이블 텔레비전 시스템, 광고판, 대중교통 광고를 포함한 광고매체의 소유자 또는 직원에게 적용되지 않는다고 규정한다(§ 50-f. 9.).

Section 1. The civil rights law is amended by adding a new section 50-f to read as follows:

§ 50-f. Right of publicity. 1. For purposes of this section:

(...)

2. (...)

b. Any person who uses a deceased performer's digital replica in a scripted audiovisual work as a fictional character or for the live performance of a musical work shall be liable for any damages sustained by the person or persons injured as a result thereof if the use occurs without prior consent from the person or persons in subdivision four of this section, if the use is likely to deceive the public into thinking it was authorized by the person or persons specified in subdivision four of this section. A use shall not be considered likely to deceive the public into thinking it was authorized by the person or persons specified in subdivision four of this section if the person making such use provides a conspicuous disclaimer in the credits of the scripted audiovisual work, and in any related advertisement in which the digital replica appears, stating that the use of the digital replica has not been authorized by the person or persons specified in subdivision four of this section.

(...)

9. Nothing in this section shall apply to the owners or employees of any medium used for advertising, including, but not limited to, newspapers, magazines, radio and television networks and stations, cable television systems, billboards, and transit advertisements, by whom any advertisement or solicitation in violation of this section is published or disseminated, unless it is established that the owners or employees had actual knowledge by prior notification of the unauthorized use of the deceased performer's digital replica or deceased personality's name, voice, signature, photograph, or likeness as prohibited by this section.

(...)

한편, 본 법은 "depicted individual(묘사된 개인)"을 digitization(디지털화)의 결과로, 실제로 수행하지 않은 수행을 제공하거나 묘사된 개인이 실제로 수행했지만 이후에 본 법안을 위반한 것으로 변경된 수행을 나타내는 것으로 보이는 개인이라고 정의하고(§ 52-c a.) "digitization(디지털화)"을 컴퓨터로 생성한, 다른 사람의 누드 신체 부위를 depicted individual(묘사된 개인)의 누드 신체 부위처럼 실제같이 묘사한 것이라고 정의하며(§ 52-c b.), "sexually explicit material(성적으로 노골적인 자료)"을 depicted individual(묘사된 개인)이 누드로 공연하는 시청각 저작물이라고 정의한다(§ 52-c e.).

Section 1. The civil rights law is amended by adding a new section 50-f to read as follows:

§ 52-c. Private right of action for unlawful dissemination or publication of a sexually explicit depiction of an individual. 1. For the purposes of this section:

a. "depicted individual" means an individual who appears, as a result of digitization, to be giving a performance they did not actually perform or to be performing in a performance that was actually performed by the depicted individual but was subsequently altered to be in violation of this section.

b. "digitization" means to realistically depict the nude body parts of another human being as the nude body parts of the depicted individual, computer-generated nude body parts as the nude body parts of the depicted individual or the depicted individual engaging in sexual conduct, as defined in subdivision ten of section 130.00 of the penal law, in which the depicted individual did not engage.

(...)

e. "sexually explicit material" means any portion of an audio visual work that shows the depicted individual performing in the nude, meaning with an unclothed or exposed intimate part, as defined in section 245.15 of the penal law, or appearing to engage in, or being subjected to, sexual conduct, as defined in subdivision ten of section 130.00 of the penal law.

(...)

위 법은 depicted individual(묘사된 개인)은 성적으로 노골적인 내용에 대한 일반적인 설명과 그것이 포함될 시청각 저작물을 포함하는 평범한 언어로 작성된 계약을 고의적으로 그리고 자발적으로 서명함으로써 성적으로 노골적인 자료의 생성, 공개, 배포 또는 출판에 동의할 수 있다는 것을 규정한다(§ 52-c 3. a.). 즉 개인이 sexually explicit material(성적으로 노골적인 자료)을 생성, 공개, 배포, 출판하는 것을 동의할 권리를 갖는다는 점을 규정하는 것이다.

Section 1. The civil rights law is amended by adding a new section 50-f to read as follows:

§ 52-c. Private right of action for unlawful dissemination or publication of a sexually explicit depiction of an individual. 1. For the purposes of this section:

3. a. A depicted individual may only consent to the creation, disclosure, dissemination, or publication of sexually explicit material by knowingly and voluntarily signing an agreement written in plain language that includes a general description of the sexually explicit material and the audiovisual work in which it will be incorporated.

또한 ① 불법활동을 보고하거나, 청문회, 재판 기타 법적 절차를 진행하는 과정에서 성적으로 노골적인 자료를 공개하거나 ② 합법적인 대중의 관심사, 정치적·뉴스적 가치 있는 저작물 또는 뉴욕주·미국 헌법에 의해 보호되는 논평 등에 의하여 성적으로 노골적인 자료를 공개하는 경우에는 책임을 지지 않는다고 규정한다(§ 52-c 4.).

Section 1. The civil rights law is amended by adding a new section 50-f to read as follows:

§ 52-c. Private right of action for unlawful dissemination or publication of a sexually explicit depiction of an individual. 1. For the purposes of this section:

4. a. A person is not liable under this section if:

i. the person discloses, disseminates or publishes the sexually explicit material in the course of reporting unlawful activity, exercising the person's law enforcement duties, or hearings, trials or other legal proceedings; or

ii. the sexually explicit material is a matter of legitimate public concern, a work of political or newsworthy value or similar work, or commentary, criticism or disclosure that is otherwise protected by the constitution of this state or the United States; provided that sexually explicit material shall not be considered of newsworthy value solely because the depicted individual is a public figure.

(...)

2.2.2. 버지니아 주

2019년 버지니아 주에서 Marcus B. Simon과 Adam P. Ebbin이 발의한 '타인 이미지의 불법 배포 또는 판매에 관한 법(Unlawful Dissemination or Sale of Images of

Another Person)'은 2019. 7. 1.부터 시행되었다.

위 법은 버지니아 코드(Virginia Code) §18.2-386.2를 개정하는 법안으로 합의하지 않은 채 "허위로 만든" 포르노 비디오 및 사진을 유포하는 경우 1급 경범죄에 해당하도록 함으로서 딥페이크 기술을 사용한 비디오 및 사진 등이 성적인 내용을 포함할시 해당 비디오 및 사진을 만들어낸 사람을 처벌할 수 있도록 하였다(Va Code Ann. §18.2-386.2, A.). 1급 경범죄의 경우 징역 1년 이하와 2,500달러의 벌금에 처해질 수 있다.

Virginia Code Title 18.2 Crimes and Offenses Generally
§18.2-386.2.

A. Any person who, with the intent to coerce, harass, or intimidate, maliciously disseminates or sells any videographic or still image created by any means whatsoever, including a falsely created videographic or still image, that depicts another person who is totally nude, or in a state of undress so as to expose the genitals, pubic area, buttocks, or female breast, where such person knows or has reason to know that he is not licensed or authorized to disseminate or sell such videographic or still image is guilty of a Class 1 misdemeanor. For purposes of this subsection, "another person" includes a person whose image was used in creating, adapting, or modifying a videographic or still image with the intent to depict an actual person and who is recognizable as an actual person by the person's face, likeness, or other distinguishing characteristic.

다만 위 법은 위 범죄 행위가 이루어진 인터넷 서비스 제공자 등에 대하여는 처벌을 면제한다는 조항을 두어 서비스 제공자는 명시적으로 면책한다(Va Code Ann. §18.2-386.2, B.).

B. If a person uses services of an Internet service provider, an electronic mail service provider, or any other information service, system, or access software provider that provides or enables computer access by multiple users to a computer server in committing acts prohibited under this section, such provider shall not be held responsible for violating this section for content provided by another person.

2.2.3. 텍사스 주

텍사스 주는 Bryan Hughes와 Royce West가 '선거 결과에 영향을 미치려는 의도로 기만적 동영상을 조작한 범죄와 관련한 법(Relating to the creation of a criminal offense for fabricating a deceptive video with intent to influence the outcome of an election)'이라는 제목으로 발의한 선거법(Election Code) 개정 법안을 2019. 6. 14. 상원의원에서 통과시켰으며, 위 법은 2019. 9. 1.부터 시행되고 있다.

위 법은 '딥페이크 비디오'를 속일 의도로 만들어진 동영상이라고 규정하며 실제 사람이 실제로 일어나지 않은 행동을 하는 것을 묘사하는 것이라고 정한다(SEC. 255.004. (e)). 또한 선거 후보자에게 영향을 미칠 의도로 (1) 딥페이크 비디오를 제작하는 경우, (2) 딥페이크 동영상이 선거일 전 30일 이내에 게시 또는 배포되도록 하는 경우에는 A급 경범죄가 성립하도록 규정한다(SEC. 255.004. (d)-(2)). A급 경범죄는 텍사스의 경범죄 혐의 중 가장 중한 형으로, 카운티 교도소에서 1년 이하의 징역과 4,000달러 이하의 벌금에 처해진다⁵¹⁾(Texas Penal Code, Title 3., Chapter12, Subchapter B, Section 12.21.).

ELECTION CODE
TITLE 15. REGULATING POLITICAL FUNDS AND CAMPAIGNS
CHAPTER 255. REGULATING POLITICAL ADVERTISING AND CAMPAIGN COMMUNICATIONS
Sec. 255.004. TRUE SOURCE OF COMMUNICATION.

51) Texas Penal Code, Title 3., Chapter12, Subchapter B, Section 12.21.

CLASS A MISDEMEANOR. An individual adjudged guilty of a Class A misdemeanor shall be punished by:

- (1) a fine not to exceed \$4,000;
- (2) confinement in jail for a term not to exceed one year; or
- (3) both such fine and confinement.

- (a) A person commits an offense if, with intent to injure a candidate or influence the result of an election, the person enters into a contract or other agreement to print, publish, or broadcast political advertising that purports to emanate from a source other than its true source.
- (b) A person commits an offense if, with intent to injure a candidate or influence the result of an election, the person knowingly represents in a campaign communication that the communication emanates from a source other than its true source.
- (c) An offense under this section is a Class A misdemeanor.
- (d) A person commits an offense if the person, with intent to injure a candidate or influence the result of an election:
- (1) creates a deep fake video; and
- (2) causes the deep fake video to be published or distributed within 30 days of an election.
- (e) In this section, "deep fake video" means a video, created with the intent to deceive, that appears to depict a real person performing an action that did not occur in reality.

2.2.4. 매사추세츠 주

매사추세츠 주는 '범죄 또는 고통을 주는 행위를 용이하게 하기 위해 사용되는 딥페이크를 방지하는 법안(An Act to Protect Against Deep Fakes Used to Facilitate Criminal or Torturous Conduct) (Mass. H. 3366)⁵²⁾'의 도입을 추진하고 있다.

위 법안은 2019. 1. 제출되었고, 본 법안에 관한 공청회가 2019. 5.에 열렸으며, 현재 사법부의 주 위원회에 계류 중이다⁵³⁾.

본 법안은 '시청각 기록(Audiovisual record)'을 '전자적 형식의 모든 청각적, 시각적

52) <https://malegislature.gov/Bills/191/H3366.Html>

53) https://www.wilmerhale.com/-/media/files/shared_content/editorial/publications/wh_publications/client_alert_pdfs/20190925-deepfake-legislation-a-nationwide-survey.pdf 중 13p 참조.

미디어로써 사진, 영화 필름, 비디오 녹화, 전자 이미지 또는 녹음을 포함한다'고 정의하고, '딥페이크(Deep fake)'를 '합리적인 관찰자에게 기록이 거짓으로 나타나 개인의 실제 언행이나 행위의 진정성 있는 기록으로 나타나는 방식으로 생성되거나 변형된 시청각 기록'이라고 정의한다(Section 37E 1/2. (a)).

SECTION 1. Chapter 266 of the General Laws is hereby amended by inserting after section 37E the following section:—

Section 37E 1/2.

(a)As used in this section, the following words shall have the following meaning unless the context clearly requires otherwise:

“Audiovisual record,” any audio or visual media in an electronic format and includes any photograph, motion-picture film, video recording, electronic image, or sound recording.

“Deep fake”, an audiovisual record created or altered in a manner that the record would falsely appear to a reasonable observer to be an authentic record of the actual speech or conduct of an individual.

또한 본 법안은 누구든지 ① 딥페이크를 배포하려는 의도 및 그 딥페이크를 배포하는 것이 범죄나 고통을 주는 행위를 용이하게 할 것이라는 의도를 가지고 딥페이크를 생성하거나 ② 시청각 기록이 딥페이크라는 사실을 알고, 시청각 기록을 배포하는 것이 범죄나 고통을 주는 행위를 용이하게 할 것이라는 의도를 가지고 시청각 기록을 배포하는 경우에는 신원 사기 범죄(crime of identity fraud)의 유죄이고, 5,000달러 이하의 벌금형 또는 2년 6월 이하의 징역형 또는 5,000달러 이하의 벌금형과 2년 6월 이하의 징역형의 병과형에 처해진다고 규정한다(Section 37E 1/2. (b)). 그리고 본 법안은 매사추세츠 헌법 또는 미국 헌법 제1차 개정에 의해 보호되는 모든 활동을 책임에서 배제한다고 규정한다(Section 37E 1/2. (b)).

SECTION 1. Chapter 266 of the General Laws is hereby amended by inserting after section 37E the following section:—

Section 37E 1/2.

(b) Whoever (1), creates, with the intent to distribute, a deep fake and with the intent that the distribution of the deep fake would facilitate criminal or tortious conduct, or (2) distributes an audiovisual record with actual knowledge that the audiovisual record is a deep fake and with the intent that the distribution of the audiovisual record would facilitate criminal or tortious conduct shall be guilty of the crime of identity fraud and shall be punished by a fine of not more than \$5,000 or imprisonment in a house of correction for not more than two and one-half years, or by both such fine and imprisonment. No person shall be held liable under this section for any activity protected by the Massachusetts Constitution or by the First Amendment to the Constitution of the United States.

본 법안의 특징적인 부분은 이미 금지된 행위를 용이하게 하기 위해 딥페이크를 사용하려는 의도에 책임이 달려있다는 점이다. 즉, 본 법안은 이미 금지된 행위에 딥페이크가 근본적으로 편승함으로써, 딥페이크를 위한 추가적인 목적(리벤지포르노, 부정선거에 선거에 영향을 미치는 것 등)을 규정하는 것을 피한다는 특징이 있다.

2.2.5. 캘리포니아 주

2019. 10. 3. 캘리포니아 주의 개빈 뉴섬(Gavin Newsom) 주지사가, 버지니아와 텍사스를 따라 'AB-602 디지털 또는 전자 기술을 이용한 개인 묘사: 성적으로 노골적인 소재: 청구원인(AB-602 Depiction of individual using digital or electronic technology: sexually explicit material: cause of action, AB-602 법)'⁵⁴⁾와 'AB-730 선거: 기만적인 오디오 또는 시각적 미디어(AB-730 Elections: deceptive audio or visual media, AB-730 법)'⁵⁵⁾에 서명하여, 두 가지 법이 모두 시행중이다.

AB-602 법은 '딥페이크'라는 용어를 명시적으로 사용하고 있지는 않으나, 캘리포니

54) https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201920200AB602

55) https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201920200AB730

아주 주민들이 그들의 사진이나 영상이 성적으로 노골적인 콘텐츠에 악용될 경우 소송을 제기할 수 있도록 하고 있다. 이 법은 피해자가 승소할 경우, 금지명령구제를 신청할 수 있고 변호사 수임료 및 비용을 회수할 수 있도록 하는 안을 담고 있다 (SECTION 1. 1708.86.(e))⁵⁶⁾.

SECTION 1. Section 1708.86 is added to the Civil Code, to read:
1708.86.

(e) (1) A prevailing plaintiff who suffers harm as a result of the violation of subdivision (b) may recover any of the following:

(A) An amount equal to the monetary gain made by the defendant from the creation, development, or disclosure of the sexually explicit material.

(B) One of the following:

(i) Economic and noneconomic damages proximately caused by the disclosure of the sexually explicit material, including damages for emotional distress.

(ii) Upon request of the plaintiff at any time before the final judgment is rendered, the plaintiff may instead recover an award of statutory damages for all unauthorized acts involved in the action, with respect to any one work, as follows:

(I) A sum of not less than one thousand five hundred dollars (\$1,500) but not more than thirty thousand dollars (\$30,000).

(II) If the unlawful act was committed with malice, the award of statutory damages may be increased to a maximum of one hundred fifty thousand dollars (\$150,000).

(C) Punitive damages.

(D) Reasonable attorney's fees and costs.

(E) Any other available relief, including injunctive relief.

(2) The remedies provided by this section are cumulative and shall not be construed as restricting a remedy that is available under any other law.

AB-730 법은 선거일⁵⁷⁾ 기준 60일 이내(Within 60 days of an election)에 특정 후보를 대상으로 악의적으로 조작 또는 변조한 동영상, 이미지 또는 오디오를 제작하거나

56) <http://www.aitimes.com/news/articleView.html?idxno=120085>

57) 일반적으로 선거일(election day)의 뜻은 'the day when people vote in an election'이며, 선거일은 투표일과 동일한 의미로 해석된다.

배포하는 행위는 불법에 해당한다고 규정하여 선거 결과에 영향을 미치는 행위를 금지한다(SEC.4. 20010.(a)). 다만 영상이 가짜로 제작된 것을 명시하는 경우에는 적용이 제외된다(SEC.4. 20010.(d)(4)).

SEC. 4. Section 20010 is added to the Elections Code, to read:
20010. (a) Except as provided in subdivision (b), a person, committee, as defined in Section 82013 of the Government Code, or other entity shall not, within 60 days of an election at which a candidate for elective office will appear on the ballot, distribute, with actual malice, materially deceptive audio or visual media, as defined in subdivision (e), of the candidate with the intent to injure the candidate's reputation or to deceive a voter into voting for or against the candidate.
(d)
(4) This section does not apply to an internet website, or a regularly published newspaper, magazine, or other periodical of general circulation, including an internet or electronic publication, that routinely carries news and commentary of general interest, and that publishes materially deceptive audio or visual media prohibited by this section, if the publication clearly states that the materially deceptive audio or visual media does not accurately represent the speech or conduct of the candidate

이 법안은 '물질적으로 기만적인 오디오 또는 시각적 미디어(materially deceptive audio or visual media)'라는 용어를 사용하여, 후보자 외관, 연설 또는 행동의 이미지 또는 비디오 녹음으로서 진짜인 것처럼 보이도록 하여, 합리적인 사람으로 하여금 다른 이해 또는 인상을 갖도록 하는, 의도적으로 조작된 것을 의미한다고 정하고 있다(SEC.4. 20010.(e)).

SEC. 4. Section 20010 is added to the Elections Code, to read:
20010.
(e) As used in this section, "materially deceptive audio or visual media" means an image or an audio or video recording of a candidate's appearance, speech, or conduct that has been intentionally manipulated in a manner such that both of the following conditions are met:

- (1) The image or audio or video recording would falsely appear to a reasonable person to be authentic.
- (2) The image or audio or video recording would cause a reasonable person to have a fundamentally different understanding or impression of the expressive content of the image or audio or video recording than that person would have if the person were hearing or seeing the unaltered, original version of the image or audio or video recording.

공직 후보자는 선거와 관련하여 "이 그림은 사실의 정확한 표현이 아니다(This picture is not an accurate representation of fact)."라는 경고 표시없이 '실제 악의적(actual malice)' 선거 관련 딥 페이크를 배포하는 개인 또는 단체에 대하여, 해당 자료의 게시, 배포, 방송을 금지하는 가처분 및 임시 금지명령을 신청할 수 있고, 민사상 손해배상청구를 할 수 있다(SEC.3. 20010.(b)).

2.2.6. 메릴랜드 주

2020. 1. 16. 메릴랜드 주는 딥 페이크에 관한 법안인 '선거법-온라인 캠페인 자료 - 딥페이크 사용(Election Law - Online Campaign Material - Use of Deepfakes)'⁵⁸⁾을 발표하였고, 2020. 2. 6. 청문회가 진행되었으나, 현재 기간만료로 폐기되었다.

이 법안은 딥페이크의 정의를 '① 캠페인 자료에 관한 것이거나, ② 컴퓨터 생성 소프트웨어(computer-generated software)에 의해 강화 또는 변경되거나, ③ 강화 또는 변경되지 않고 동작 묘사, 소리, 또는 발성을 묘사한' 오디오 녹음·비디오 녹음·사진이라고 정하고 있다(13-401.1(A).(2)).

13-401.1.

INDICATED.

(2) "DEEPFAKE" MEANS AN AUDIO RECORDING, A VIDEO RECORDING, OR A P

58) <https://www.billtrack50.com/BillDetail/1174065>

PHOTOGRAPH THAT:

(I) IS CAMPAIGN MATERIAL

(II) IS ENHANCED OR OTHERWISE ALTERED BY COMPUTER-GENERATED SOFTWARE AND

(III) DEPICTS AN ACTION, A SOUND, OR A VOCALIZATION THAT DID NOT OCCUR AS ENHANCED OR OTHERWISE ALTERED.

이 법안은 선거일⁵⁹⁾로부터 90일 이전(Within 90 days before an election)에 온라인에 딥페이크를 게시, 배포함으로써 유권자들이 특정 후보에 대하여 투표하는 것에 고의로 영향을 미치거나 미치려는 것을 금지하고 있다(13-401.1(C)(1)). 다만 오디오 녹음, 비디오 녹화 또는 사진의 내용이 변경되었다는 정보 등 딥페이크에 대한 특정 정보를 명확하고 눈에 띄는 방식으로 공개한 경우에는 해당 조항이 적용되지 않는다(13-401.1(C)(2)).

13-401.1.

(C) (1) EXCEPT AS PROVIDED IN PARAGRAPH (2) OF THIS SUBSECTION, A PERSON SUBJECT TO THIS SECTION MAY NOT WILLFULLY OR KNOWINGLY INFLUENCE OR ATTEMPT TO INFLUENCE A VOTER'S DECISION TO GO TO THE POLLS OR TO CAST A VOTE FOR A PARTICULAR CANDIDATE BY PUBLISHING, DISTRIBUTING, OR DISSEMINATING A DEEPFAKE ONLINE WITHIN 90 DAYS BEFORE AN ELECTION.

(2) PARAGRAPH (1) OF THIS SUBSECTION DOES NOT APPLY TO A PERSON WHO DISCLOSES, IN A CLEAR AND CONSPICUOUS MANNER AT THE BEGINNING OF THE AUDIO RECORDING OR VIDEO RECORDING OR ON THE PHOTOGRAPH:

13-401.1를 위반하여 경범죄 유죄판결을 받는 경우, 5,000달러 이하의 벌금 또는 1년 이하의 징역형에 처해질 수 있다(13-602(b)(1)(II)).

59) 일반적으로 선거일(election day)의 뜻은 'the day when people vote in an election'이며, 선거일은 투표일과 동일한 의미로 해석된다.

13-602.

(b) A person who violates this section is guilty of a misdemeanor and on conviction is:

(1) (II) FOR A VIOLATION RELATED TO § 13-401.1 OF THIS SUBTITLE, SUBJECT TO A FINE NOT EXCEEDING \$5,000 OR IMPRISONMENT NOT EXCEEDING 1 YEAR OR BOTH AND

2.2.7. 미시간 주

미시간 주는 딥페이크만을 위한 법안을 발의한 것은 아니며 기존에 있던 형사법인 '사이버스토킹법'을 통해 딥페이크를 규제하고 있다. 사이버스토킹법은 미국 미시간 주 형법(The Michigan Penal Code (Excerpt)Act 328 of 1931)⁶⁰⁾ 내에 있는 제750.411s조를 뜻한다. 해당 조항은 2000년 제정되었으며, 2001년 시행되었다.

위 법은 '피해자가 공포, 겁, 협박, 위협, 희롱 또는 성희롱을 느끼게 하는 행동을 유발하기 위한 메시지를 피해자의 동의 없이 인터넷 등 게시해서는 안 된다'고 규정하고 있다(제750.411s조 (1)). 이때 메시지에는 허위의 메시지가 포함된다(동법 (8)(i)).

THE MICHIGAN PENAL CODE (EXCERPT)

Act 328 of 1931

750.411s Posting message through electronic medium; prohibitions; penalty; exceptions; definitions.

Sec. 411s.

(1) A person shall not **post a message** through the use of any medium of communication, including the internet or a computer, computer program, computer system, or computer network, or other electronic medium of communication, without the victim's consent, if all of the following apply:

(a) The person knows or has reason to know that posting the message could cause 2 or more separate noncontinuous acts of unconsented contact with the victim.

(b) Posting the message is intended to cause conduct that would make the victim fe

60) 제750.411s조가 위치한 미국 미시간 주 형법은 1931년 제정되었다.

el terrorized, frightened, intimidated, threatened, harassed, or molested.

(c) Conduct arising from posting the message would cause a reasonable person to suffer emotional distress and to feel terrorized, frightened, intimidated, threatened, harassed, or molested.

(d) Conduct arising from posting the message causes the victim to suffer emotional distress and to feel terrorized, frightened, intimidated, threatened, harassed, or molested.

(8) As used in this section:

(i) "Post a message" means transferring, sending, posting, publishing, disseminating, or otherwise communicating or attempting to transfer, send, post, publish, disseminate, or otherwise communicate information, whether truthful or untruthful, about the victim.

제750.411s조 제(1)항에서 금지하는 행위를 한 가해자는 2년 이하의 징역 또는 5,000달러 이하의 벌금형에 처해지며(동법 (1)), 법원은 동법 위반으로 인하여 유죄판결을 받은 사람에게 주(state) 또는 지방자치단체(a local unit of government)에 대하여 동법위반으로 인하여 발생한 비용을 상환하도록 명할 수 있다고 규정하고 있다(동법 (4)). 한편, 위 법은 선의로 또는 게시된 메시지의 특정 특성을 알지 못하고, 사람들 사이 정보나 소통을 전파하는 매체를 제공하는 인터넷 또는 컴퓨터 네트워크 서비스 제공업체에 대하여는 책임을 묻지 않는다(동법 (3)).

THE MICHIGAN PENAL CODE (EXCERPT)

Act 328 of 1931

(2) A person who violates subsection (1) is guilty of a crime as follows:

(a) Except as provided in subdivision (b), the person is guilty of a felony punishable by imprisonment for not more than 2 years or a fine of not more than \$5,000.00, or both.

(b) 생략

(3) This section does not apply to an internet or computer network service provider who in good faith, and without knowledge of the specific nature of the message posted, provides the medium for disseminating information or communication between persons.

(4) The court may order a person convicted of violating this section to reimburse this state or a local unit of government of this state for the expenses incurred in relation to the violation in the same manner that expenses may be ordered to be reimbursed under section 1f of chapter IX of the code of criminal procedure, 1927 PA 175, MCL 769.1f..

2.3. 소결

연방차원에서 새로 입법이 추진되고 있는 법률들은 딥페이크를 독립적으로 다루는 법안들로서 딥페이크의 정의, 예외규정, 형사처벌, 민사배상, 플랫폼 사업자의 책임, 담당부처, 보고서 작성의무, 공청회 개최의무, 딥페이크 표시의무 부과 등 상당히 구체적인 내용을 담고 있으나, 아직 입법이 완료되지 않아 본격적으로 시행되지는 않고 있다. 미국 주차원에서의 법률은 각 주의 실정에 맞게 특화되어 입법되었으며 상당수는 현재 시행되고 있다.

3. EU 및 유럽국가

3.1. EU

EU는 이미 시행하고 있는 개인정보보호규정(GDPR, General Data Protection Regulation)에 의하여 딥페이크 피해자에 대한 보호가 가능하다.

딥페이크 피해자는 GDPR 제17조의 삭제권(잊힐 권리)에 따라 딥페이크에 악용된 자신의 개인정보에 대하여 삭제를 요구할 권리가 있다. 이에 따르면 정보주체는 동의 철회시 또는 정보사회서비스의 제공과 관련하여 개인정보 수집이 이루어진 경우 등과 같은 특정 사유가 존재할 경우에 삭제권을 행사할 수 있다. GDPR상의 삭제권의 가장

큰 특징은, 해당 컨트롤러(개인정보처리자)가 만약 그 개인정보를 공개한 경우라면, 그 컨트롤러는 스스로만 삭제의무를 이행하면 족한 것이 아니라, 그 개인정보를 처리하는 다른 컨트롤러들에게, 해당 정보주체가 그 개인정보의 일체의 링크 또는 사본이나 복제본의 삭제를 요청하였음을 알리기 위하여 기술적 조치를 포함한 합리적인 조치를 취하도록 의무를 부과하고 있다는 점이다.

삭제권(“잊힐 권리”)(GDPR 제17조)

제17조 삭제권(“잊힐 권리”)

1. 정보주체는 컨트롤러로부터 자신에 관한 개인정보의 삭제를 부당한 지체 없이 얻을 권리를 가지며, 컨트롤러는 다음의 근거가 적용되는 경우 부당한 지체 없이 개인정보를 삭제할 의무를 가진다:

- (a) 개인정보가 수집된 목적 또는 기타 처리된 목적과 관련하여 더 이상 필요하지 않은 경우;
- (b) 정보주체가 제6조 제1항 (a)호 또는 제9조 제2항 (a)호에 따른 처리의 근거가 되는 동의를 철회하고, 그 처리에 대한 다른 법적 근거가 없는 경우;
- (c) 정보주체가 제21조 제1항에 따라 처리를 반대하고 그 처리에 대해 우선하는 정당한 근거가 없는 경우, 또는 정보주체가 제21조 제2항에 따라 처리를 반대하는 경우;
- (d) 개인정보가 불법적으로 처리된 경우;
- (e) 컨트롤러에게 적용되는 EU 또는 회원국 법의 법적 의무를 준수하기 위하여 그 개인정보가 삭제되어야 하는 경우;
- (f) 개인정보가 제8조 제1항에서 언급된 정보사회서비스의 제공과 관련하여 수집된 경우.

2. 컨트롤러가 개인정보를 공개하였고 제1항에 따라 그 개인정보를 삭제할 의무가 있는 경우, 컨트롤러는, 이용가능한 기술과 이행비용을 고려하여 그 개인정보를 처리하는 컨트롤러들에게, 해당 정보주체가 그 개인정보의 일체의 링크 또는 사본이나 복제본의 컨트롤러들에 의한 삭제를 요청하였음을 알리기 위하여 기술적 조치를 포함한 합리적인 조치를 취하여야 한다.

3. 제1항 및 제2항은 다음을 위하여 처리가 필요한 경우에는 적용되지 아니한다:

- (a) 표현과 정보의 자유권 행사를 위한 경우;
- (b) 컨트롤러에게 적용되는 EU 또는 회원국 법에 의해 처리가 요구되는 법적 의무의 준수 또는 공익상 수행되는 직무의 실행을 위하여나 컨트롤러에게 부여된 공식 권한의 행사를 위한 경우;
- (c) 제9조 제2항 (h)호, (i)호 및 제9조 제3항에 따른 공중보건 분야의 공익상 이유를 위한 경우;

- (d) 제89조 제1항을 준수한 공익적 기록 보존 목적, 과학적 또는 역사적 연구 목적 또는 통계적 목적을 위한 경우로서 제1항에 언급된 권리가 처리 목적의 달성을 불가능하게 하거나 심각하게 저해할 것 같은 경우; 또는
- (e) 법적 청구권의 설정, 행사 또는 방어를 위한 경우.

나아가 딥페이크 피해자는 GDPR 제18조의 처리제한권에 따라 딥페이크에 악용된 자신의 개인정보에 대해서 처리의 제한을 요구할 수 있는 권리를 가지며, 컨트롤러는 개인정보의 처리 정정, 삭제, 처리제한 조치를 취하고 정보주체에게 통지하여야 한다.

처리제한권(GDPR 제18조)

제18조 처리제한권

1. 정보주체는 다음의 하나에 해당하는 경우 컨트롤러로부터 처리의 제한을 얻을 권리를 가진다:
 - (a) 정보주체가 개인정보의 정확성에 대하여 이의를 제기한 경우로서 컨트롤러가 개인정보의 정확성을 입증할 수 있는 기간 동안;
 - (b) 처리가 불법적이고 정보주체가 개인정보의 삭제에 반대하면서 대신 그 이용의 제한을 요청한 경우;
 - (c) 컨트롤러가 그 처리 목적을 위하여 그 개인정보를 더 이상 필요로 하지 않으나 정보주체가 법적 청구권의 설정, 행사 또는 방어를 위하여 해당 개인정보를 요하는 경우;
 - (d) 정보주체가 제21조 제1항에 따라 처리를 반대한 경우로서 컨트롤러의 정당한 근거가 정보주체의 정당한 근거에 우선하는지 여부가 확인될 때까지.
2. 제1항에 따라 처리가 제한된 경우, 그러한 개인정보는, 저장의 경우를 제외하고, 정보주체의 동의가 있거나 법적 청구권의 설정, 행사 또는 방어를 위하여 또는 다른 자연인이나 법인의 권리 보호를 위하여 또는 EU나 회원국의 중요한 공익을 이유로만 처리되어야 한다.
3. 제1항에 따라 처리의 제한을 얻은 정보주체는 그 처리 제한이 해제되기 전에 이를 고지받아야 한다.

제19조 개인정보의 정정이나 삭제 또는 처리제한에 관한 통지 의무

컨트롤러는 그 개인정보를 공개받은 각 수령자에게 제16조, 제17조 제1항 및 제18조에 따른 개인정보의 정정이나 삭제 또는 처리 제한을 통지하여야 하며, 다만 이러한 통지가 불가능함이 입증되거나 비례적으로 과도한 노력을 수반하는 경우는 제외된다. 컨트롤러는 정보주체가 요청한 경우 그 수령자들에 관하여 정보주체에게 고지하여야

한다.

이외에도 EU는 딥페이크에 대하여 한정되거나 독립된 것은 아니지만 허위조작정보 식별(disinformation)을 위한 각종 조치 또는 규약 등을 정하여 발표하고 있다.

2018년에 정보의 출처 및 신뢰성 여부 확인을 위한 조치(Communication-Tackling online disinformation: a European Approach)⁶¹⁾를 발표하였으며, 2018. 10. 허위조작정보 대응 행동 규약(Code of Practice on Disinformation)⁶²⁾을 제정하였다. 온라인 플랫폼 및 소셜네트워크 운영자, 광고주, 광고회사 등이 규약에 서명하였으며, 위 규약은 허위조작정보 대응 기준을 제시한 자율규제로서 의미가 있다. 또한 2018. 12. 허위조작정보에 관한 실행계획(Action Plan on Disinformation)⁶³⁾을 수립하였고, 2019. 6. 14. 허위조작정보에 대한 실행계획의 이행에 대한 보고(Report on the Implementation of the Action Plan Against Disinformation)⁶⁴⁾을 발표하여 허위정보에 대한 대응을 보다 발전시켰다.

위와 같은 조치 또는 규약은 딥페이크에 한정된 것이 아니라 허위조작정보를 포괄적으로 다루고 있다. 위 조치 또는 규약은 법적인 구속력은 갖지 않고 권고적인 효력에 머문다는 한계가 있다.

3.2. 프랑스

프랑스에서는 딥페이크에 특화된 독립된 법안이 추진되지는 아니하였으며, 허위조작정보에 대한 법을 마련하였다.

61) <https://ec.europa.eu/digital-single-market/en/news/communication-tackling-online-disinformation-european-approach>

62) <https://ec.europa.eu/digital-single-market/en/news/code-practice-disinformation>

63) https://ec.europa.eu/commission/publications/action-plan-disinformation-commission-contribution-european-council-13-14-december-2018_en

64) https://eeas.europa.eu/sites/eeas/files/joint_report_on_disinformation.pdf

프랑스는 정보조작 대처에 관한 2018. 12. 22. 법률 제2018-1202호 정보조작대처법 (LOI n° 2018-1202 du 22 decembre 2018 relative a la lutte contre la manipulation de l'information)⁶⁵⁾을 제정하였다.

프랑스는 위 정보조작대처법을 통해 선거법전(Code électoral)⁶⁶⁾을 개정하였다. 선거 기간 동안 온라인 플랫폼 사업자는 공공정책 토론과 관련된 정보콘텐츠의 광고비에 대한 정보를 온라인 플랫폼 이용자에게 제공하여야 한다(Article L 163-1). 이를 위반 하는 경우 금고 1년 또는 벌금 7만5천 유로에 처한다(Article L112).

Code électoral

Article L163-1.

Pendant les trois mois précédant le premier jour du mois d'élections générales et jusqu'à la date du tour de scrutin où celles-ci sont acquises, les opérateurs de plateforme en ligne au sens de l'article L. 111-7 du code de la consommation dont l'activité dépasse un seuil déterminé de nombre de connexions sur le territoire français sont tenus, au regard de l'intérêt général attaché à l'information éclairée des citoyens en période électorale et à la sincérité du scrutin :

1° De fournir à l'utilisateur une information loyale, claire et transparente sur l'identité de la personne physique ou sur la raison sociale, le siège social et l'objet social de la personne morale et de celle pour le compte de laquelle, le cas échéant, elle a déclaré agir, qui verse à la plateforme des rémunérations en contrepartie de la promotion de contenus d'information se rattachant à un débat d'intérêt général ;

2° De fournir à l'utilisateur une information loyale, claire et transparente sur l'utilisation de ses données personnelles dans le cadre de la promotion d'un contenu d'information se rattachant à un débat d'intérêt général ;

3° De rendre public le montant des rémunérations reçues en contrepartie de la promotion de tels contenus d'information lorsque leur montant est supérieur à un seuil déterminé.

Ces informations sont agrégées au sein d'un registre mis à la disposition du public par voie électronique, dans un format ouvert, et régulièrement mis à jour au cours

65) https://www.legifrance.gouv.fr/download/pdf?id=6-nJtAIQpD8-Ugn4wumM7q3PzXyh2U2x_naRfEud_Wg=

66) https://www.legifrance.gouv.fr/codes/texte_lc/LEGITEXT000006070239/2020-09-17/

de la période mentionnée au premier alinéa du présent article.

Les modalités d'application du présent article sont définies par décret.

Article L112

Toute infraction aux dispositions de l'article L. 163-1 est punie d'un an d'emprisonnement et de 75 000 € d'amende.

Les personnes morales déclarées responsables pénalement, dans les conditions prévues à l'article 121-2 du code pénal, de l'infraction définie au premier alinéa du présent article encourent, outre l'amende suivant les modalités prévues à l'article 131-38 du même code, les peines prévues aux 2° et 9° de l'article 131-39 dudit code. L'interdiction prévue au 2° du même article 131-39 est prononcée pour une durée de cinq ans au plus et porte sur l'activité professionnelle dans l'exercice ou à l'occasion de laquelle l'infraction a été commise.

선거기간 동안 특정 사실에 대해 부정확하거나 오해소지가 있는 주장이 온라인 공공정보 통신서비스를 통해 고의 또는 자동으로 대량 유포되는 경우, 가처분 전담판사는 검찰, 후보자, 정당, 정치집단 등의 요청에 따라 해당 정보의 유포를 중단시키기 위한 조치를 취하도록 명할 수 있다(Article L163-2).

Code électoral

Article L163-2

I. - Pendant les trois mois précédant le premier jour du mois d'élections générales et jusqu'à la date du tour de scrutin où celles-ci sont acquises, lorsque des allégations ou imputations inexactes ou trompeuses confient dans l'économie numérique ou, à défaut, à toute personne mentionnée au 1 du même I toutes mesures proportionnées et nécessaires pour faire cesser cette diffusion.

II. - Le juge des référés se prononce dans un délai de quarante-huit heures à compter d'un fait de nature à altérer la sincérité du scrutin à venir sont diffusées de manière délibérée, artificielle ou automatisée et massive par le biais d'un service de communication au public en ligne, le juge des référés peut, à la demande du ministère public, de tout candidat, de tout parti ou groupement politique ou de toute personne ayant intérêt à agir, et sans préjudice de la réparation du dommage subi, prescrire aux personnes physiques ou morales mentionnées au 2 du I de l'article 6 de la loi n° 2004-575 du 21 juin 2004 pour la de la saisine.

En cas d'appel, la cour se prononce dans un délai de quarante-huit heures à compt

er de la saisine.

III.—Les actions fondées sur le présent article sont exclusivement portées devant un tribunal de grande instance et une cour d'appel déterminés par décret.

정보조작대처법은 정보통신자유에 관한 1986. 9. 30. 법률 제86-1067호(LOI n° 86-1067 du 30 septembre 1986 relative a la liberte de communication)⁶⁷⁾을 개정하였다. 위 법에 따라 선거 및 국민투표 기간 동안 허위조작정보가 유포된 경우, 시청각고등위원회(Conseil superieur de l'audiovisuel)는 외국의 통제를 받거나 외국의 영향력 하에 있는 법인과 체결된 협약 대상이 되는 라디오 또는 텔레비전 서비스의 유포를 중단할 수 있다(Article 33-1-1).

Loi n° 86-1067 du 30 septembre 1986 relative à la liberté de communication

Article 33-1-1

Pendant les trois mois précédant le premier jour du mois de l'élection du Président de la République, des élections générales des députés, de l'élection des sénateurs, de l'élection des représentants au Parlement européen et des opérations référendaires, et jusqu'à la date du tour de scrutin où ces élections sont acquises, le Conseil supérieur de l'audiovisuel, s'il constate que le service ayant fait l'objet d'une convention conclue avec une personne morale contrôlée, au sens de l'article L. 233-3 du code de commerce, par un Etat étranger ou placée sous l'influence de cet Etat diffuse, de façon délibérée, de fausses informations de nature à altérer la sincérité du scrutin, peut, pour prévenir ou faire cesser ce trouble, ordonner la suspension de la diffusion de ce service par tout procédé de communication électronique jusqu'à la fin des opérations de vote.

정보조작대처법은 선거법전 Article L 163-1에 규정된 온라인 플랫폼 운영자로 하여금 공공질서를 침해하거나 정보통신자유에 관한 1986. 9. 30. 법률 제86-1067호 Article 33-1-1에 규정된 투표의 진정성을 해칠 수 있는 허위정보의 보급에 대처하기 위한 조치를 취하도록 하고 있다. 온라인 플랫폼 사업자는 특히 제3자가 업로드한 콘

67) <https://www.legifrance.gouv.fr/loda/id/LEGITEXT000006068930/2020-09-17/>

텐츠에서 유래한 정보를 이용자가 제보할 수 있도록 쉽게 접근할 수 있도록 눈에 띄는 장치를 설정해야 하며, 플랫폼 알고리즘의 투명성 확보, 허위정보를 대량으로 유포하는 계정에 대한 대처, 콘텐츠의 본질, 출처 및 확산 방법에 관한 이용자의 정보확보, 미디어 및 정보교육 등의 보완조치를 시행하여야 한다(Article 11). 온라인 플랫폼 사업자는 위 조치의 이행수단을 공개하고, 이행한 내역에 대한 신고를 시청각고등위원회에 제출하여야 한다(Article 11).

LOI n° 2018-1202 du 22 décembre 2018 relative à la lutte contre la manipulation de l'information

Article 11

I. – Les opérateurs de plateforme en ligne mentionnés au premier alinéa de l'article L. 163-1 du code électoral mettent en œuvre des mesures en vue de lutter contre la diffusion de fausses informations susceptibles de troubler l'ordre public ou d'altérer la sincérité d'un des scrutins mentionnés au premier alinéa de l'article 33-1-1 de la loi n° 86-1067 du 30 septembre 1986 relative à la liberté de communication.

Ils mettent en place un dispositif facilement accessible et visible permettant à leurs utilisateurs de signaler de telles informations, notamment lorsque celles-ci sont issues de contenus promus pour le compte d'un tiers.

Ils mettent également en œuvre des mesures complémentaires pouvant notamment porter sur :

- 1° La transparence de leurs algorithmes ;
- 2° La promotion des contenus issus d'entreprises et d'agences de presse et de services de communication audiovisuelle ;
- 3° La lutte contre les comptes propageant massivement de fausses informations ;
- 4° L'information des utilisateurs sur l'identité de la personne physique ou la raison sociale, le siège social et l'objet social des personnes morales leur versant des rémunérations en contrepartie de la promotion de contenus d'information se rattachant à un débat d'intérêt général ;
- 5° L'information des utilisateurs sur la nature, l'origine et les modalités de diffusion des contenus ;
- 6° L'éducation aux médias et à l'information.

Ces mesures, ainsi que les moyens qu'ils y consacrent, sont rendus publics. Chaque opérateur adresse chaque année au Conseil supérieur de l'audiovisuel une déclaration

dans laquelle sont précisées les modalités de mise en œuvre desdites mesures.

시청각고등위원회는 사업자의 의무이행에 대해 모니터링하고, 그 결과를 정기적으로 발행한다(Article 17-2).

Loi n° 86-1067 du 30 septembre 1986 relative à la liberté de communication

Article 17-2

Créé par LOI n°2018-1202 du 22 décembre 2018 – art. 12

Le Conseil supérieur de l'audiovisuel contribue à la lutte contre la diffusion de fausses informations susceptibles de troubler l'ordre public ou de porter atteinte à la sincérité d'un des scrutins mentionnés au premier alinéa de l'article 33-1-1 de la présente loi. En cas de nécessité, il adresse, à ce titre, aux opérateurs de plateforme en ligne mentionnés au premier alinéa de l'article L. 163-1 du code électoral des recommandations visant à améliorer la lutte contre la diffusion de telles informations. Il s'assure du suivi de l'obligation pour les opérateurs de plateforme en ligne de prendre les mesures prévues à l'article 11 de la loi n° 2018-1202 du 22 décembre 2018 relative à la lutte contre la manipulation de l'information. Il publie un bilan périodique de leur application et de leur effectivité. A cette fin, il recueille auprès de ces opérateurs, dans les conditions fixées à l'article 19 de la présente loi, toutes les informations nécessaires à l'élaboration de ce bilan.

또한 프랑스는 언론의 자유에 관한 1881. 7. 29. 법률(Loi du 29 juillet 1881 sur la liberté de la presse)⁶⁸⁾ 통해 가짜뉴스(fausses nouvelles)를 출판, 배포, 복제하여 공공의 평화를 해지거나 해칠 우려가 있는 경우 벌금 45,000 유로에 처하고 있다. 또한 온라인 플랫폼 이외 여하한의 매체를 통하여 가짜뉴스임을 알고도 출판, 배포, 복제하여 공공의 평화를 해지거나 해칠 우려가 있는 경우 벌금 135,000 유로에 처하고 있다(Article 27).

Loi du 29 juillet 1881 sur la liberté de la presse

Article 27

68) <https://www.legifrance.gouv.fr/loda/id/LEGITEXT000006070722/2020-09-17/>

La publication, la diffusion ou la reproduction, par quelque moyen que ce soit, de nouvelles fausses, de pièces fabriquées, falsifiées ou mensongèrement attribuées à des tiers lorsque, faite de mauvaise foi, elle aura troublé la paix publique, ou aura été susceptible de la troubler, sera punie d'une amende de 45 000 euros.

Les mêmes faits seront punis de 135 000 euros d'amende, lorsque la publication, la diffusion ou la reproduction faite de mauvaise foi sera de nature à ébranler la discipline ou le moral des armées ou à entraver l'effort de guerre de la Nation.

3.3. 독일

독일 또한 딥페이크에 특화된 독립된 법안이 추진되지는 아니하였으며, 위법한 콘텐츠에 대한 소셜네트워크 운영자에 대한 책임위주로 법이 마련되어 있다.

독일은 2017. 9. 1. 소셜네트워크상의 법집행 개선에 관한 법률(Gesetz zur Verbesserung der Rechtsdurchsetzung in sozialen Netzwerken, 네트워크 법집행법)⁶⁹⁾을 제정하여 2017. 10. 1.부터 시행하고 있다.

위법은 회원수가 2백만 명 이상인 소셜네트워크 운영자에게 적용된다(§ 1).

§ 1 Anwendungsbereich

(1) Dieses Gesetz gilt für Telemediendiensteanbieter, die mit Gewinnerzielungsabsicht Plattformen im Internet betreiben, die dazu bestimmt sind, dass Nutzer beliebige Inhalte mit anderen Nutzern teilen oder der Öffentlichkeit zugänglich machen (soziale Netzwerke). Plattformen mit journalistisch-redaktionell gestalteten Angeboten, die vom Diensteanbieter selbst verantwortet werden, gelten nicht als soziale Netzwerke im Sinne dieses Gesetzes. Das Gleiche gilt für Plattformen, die zur Individualkommunikation oder zur Verbreitung spezifischer Inhalte bestimmt sind.

(2) Der Anbieter eines sozialen Netzwerks ist von den Pflichten nach den §§ 2 und 3 befreit, wenn das soziale Netzwerk im Inland weniger als zwei Millionen registrierte Nutzer hat.

69) <https://www.gesetze-im-internet.de/netzdg/BJNR335210017.html>

소셜네트워크 운영자는 위법한 콘텐츠에 대해 불만처리 절차를 마련해야 하며, 위법한 콘텐츠에 대한 신고접수가 있으면 지체없이 콘텐츠의 위법성을 검토하고, 명백히 위법한 콘텐츠는 신고 접수 후 24시간 이내에 삭제 또는 접근 차단 조치하고, 그 외 위법상 콘텐츠는 원칙적으로 신고 접수 후 7시간 이내에 처리하도록 하고 있다. 또한 위와 같은 결정에 대해서 신고인 및 이용자에게 지체없이 알려야 하며, 결정의 근거를 설명하여야 한다(§ 3).

§ 3 Umgang mit Beschwerden über rechtswidrige Inhalte

(1) Der Anbieter eines sozialen Netzwerks muss ein wirksames und transparentes Verfahren nach Absatz 2 und 3 für den Umgang mit Beschwerden über rechtswidrige Inhalte vorhalten. Der Anbieter muss Nutzern ein leicht erkennbares, unmittelbar erreichbares und ständig verfügbares Verfahren zur Übermittlung von Beschwerden über rechtswidrige Inhalte zur Verfügung stellen.

(2) Das Verfahren muss gewährleisten, dass der Anbieter des sozialen Netzwerks 1.unverzüglich von der Beschwerde Kenntnis nimmt und prüft, ob der in der Beschwerde gemeldete Inhalt rechtswidrig und zu entfernen oder der Zugang zu ihm zu sperren ist,

2.einen offensichtlich rechtswidrigen Inhalt innerhalb von 24 Stunden nach Eingang der Beschwerde entfernt oder den Zugang zu ihm sperrt; dies gilt nicht, wenn das soziale Netzwerk mit der zuständigen Strafverfolgungsbehörde einen längeren Zeitraum für die Löschung oder Sperrung des offensichtlich rechtswidrigen Inhalts vereinbart hat,

3.jeden rechtswidrigen Inhalt unverzüglich, in der Regel innerhalb von sieben Tagen nach Eingang der Beschwerde entfernt oder den Zugang zu ihm sperrt; die Frist von sieben Tagen kann überschritten werden, wenn

a) die Entscheidung über die Rechtswidrigkeit des Inhalts von der Unwahrheit einer Tatsachenbehauptung oder erkennbar von anderen tatsächlichen Umständen abhängt; das soziale Netzwerk kann in diesen Fällen dem Nutzer vor der Entscheidung Gelegenheit zur Stellungnahme zu der Beschwerde geben,

b) das soziale Netzwerk die Entscheidung über die Rechtswidrigkeit innerhalb von sieben Tagen nach Eingang der Beschwerde einer nach den Absätzen 6 bis 8 anerkannten Einrichtung der Regulierten Selbstregulierung überträgt und sich deren Entscheidung

ung unterwirft,
 4. im Falle der Entfernung den Inhalt zu Beweis Zwecken sichert und zu diesem Zweck für die Dauer von zehn Wochen innerhalb des Geltungsbereichs der Richtlinien 2000/31/EG und 2010/13/EU speichert,
 5. den Beschwerdeführer und den Nutzer über jede Entscheidung unverzüglich informiert und seine Entscheidung ihnen gegenüber begründet.

규제대상이 되는 위법한 콘텐츠는 독일형법(StGB) 상 범죄에 해당하는 표현⁷⁰⁾인데, 그 중 딥페이크와 관련이 있는 것은 방송 또는 전자정보를 통한 음란물의 제공(제18조d조), 모욕(제185조), 비방(제186조), 사진촬영을 통한 사생활 영역의 침해(제201a조), 중요 증거자료의 위조(제269조) 등이 될 수 있다.

4. 호주

호주는 2018. 8. 31. 승인된 '온라인안전강화법 2018(Enhancing Online Safety Act 2018)'으로 '온라인안전강화법 2015(Enhancing Online Safety Act 2015)' 및 '형법 1995'를 개정하여 동의 없는 개인적 이미지 무단 배포 행위를 불법화하였다.

개정된 '온라인안전강화법 2015'⁷¹⁾는 개인적 이미지(intimate image)를 '당사자의 생식기 부위 또는 항문 부위(벌거벗은 상태 또는 속옷으로 덮여 있는 상태) 또는 (ii) 보

70) 제86조 위험단체 선전물 배포, 제86a조 위험단체 표시 사용, 제89a조 국가를 위협하는 중대한 폭력행위(테러행위)의 예비, 제91조 국가를 위협하는 중대한 폭력행위(테러행위)의 조장, 제100a조 간첩목적의 위조, 제111조 공연한 범죄 선동, 제126조 범죄위협에 의한 공공평온 교란, 제129조 범죄단체의 조직, 제129a조 테러단체의 조직, 제129b조 외국에서 범죄단체와 테러단체의 조직, 제130조 국민 선동, 제131조 폭력물 반포, 제140조 범죄의 대가 지급 및 찬양, 제166조 신앙, 종교단체, 세계관단체 등에 대한 모욕, 제184d조 방송 또는 전자정보를 통한 음란물의 제공(아동음란물의 배포, 취득, 소유), 제185조 모욕, 제186조 비방, 제187조 중상, 제201a 사진촬영을 통한 사생활 영역의 침해, 제241조 협박, 제269조 중요 증거자료의 위조

71) '온라인안전강화법 2018'을 통하여 '온라인안전강화법 2015'의 내용을 개정하여 현재 적용되는 개정법의 정식명칭은 여전히 '온라인안전강화법 2015'이다.

통 합리적인 사람이 프라이버시가 제공될 것으로 합리적으로 기대하는 상황에서 여성이거나 트랜스젠더 또는 여성으로 식별되는 중간 성관계자인 경우, 해당 사람의 젖가슴 또는 양쪽 모두가 나타나는 사적 이미지, 그리고 보통 합리적인 사람이 프라이버시가 제공될 것으로 합리적으로 기대하는 상황에서 옷을 벗은 상태로, 또는 (ii) 화장실 사용 (iii) 샤워 또는 (iv) 목욕, 또는 (v) 일반적으로 공공장소에서 행해지는 것이 아닌 종류의 성행위를 하는 경우, 또는 (vi) 다른 유사한 활동에 종사하는 경우를 묘사하는 사적 이미지 등을 개인적 이미지로 정의한다(SEC. 9B).

9B Intimate image

(1) This section sets out the circumstances in which material is an intimate image of a person for the purposes of this Act.

Depiction of private parts

(2) Material is an intimate image of a person if:

(a) the material consists of a still visual image or moving visual images; and

(b) the material depicts, or appears to depict:

(i) the person's genital area or anal area (whether bare or covered by underwear);

(ii) if the person is female or a transgender or intersex person identifying as female—either or both of the person's breasts;

in circumstances in which an ordinary reasonable person would reasonably expect to be afforded privacy.

Depiction of private activity

(3) Material is an intimate image of a person if:

(a) the material consists of a still visual image or moving visual images; and

(b) the material depicts, or appears to depict, the person:

(i) in a state of undress; or

(ii) using the toilet; or

(iii) showering; or

(iv) having a bath; or

(v) engaged in a sexual act of a kind not ordinarily done in public; or

(vi) engaged in any other like activity;

in circumstances in which an ordinary reasonable person would reasonably expect to

be afforded privacy.

위 법은 개인적 이미지(intimate image)를 소셜미디어, 전자기기, 인터넷 등을 사용하여 개인의 동의 없이 게시하는 경우 500벌칙 단위⁷²⁾를 부과한다(SEC. 44B).

Division 2—Intimate images must not be posted without consent etc.

44B Posting an intimate image

(1) A person (the first person) must not post, or make a threat to post, an intimate image of another person (the second person) on:

- (a) a social media service; or
- (b) a relevant electronic service; or
- (c) a designated internet service;

if:

- (d) the first person is ordinarily resident in Australia; or
- (e) the second person is ordinarily resident in Australia.

Civil penalty: 500 penalty units.

그러나 위 개인적 이미지에 딥페이크 기술을 사용하여 조작한 이미지가 포함되는지 여부에 관하여는 명확한 해석이 존재하지 아니하며 명문 해석상 포함되지 않는다고 봄이 바람직한 바, 딥페이크 기술을 사용한 이미지까지 위 규정을 사용하여 처벌하기에는 어려워 보인다.

다만 2020. 6. 23. 최종 개정된 호주의 뉴사우스웨일즈주의 형법(Crimes Act 1900)는 딥페이크 기술을 활용한 이미지를 처벌할 수 있도록 해석되는 법안이다.

위 법은 개인적 이미지(intimate image)의 동의 없는 촬영 및 유포를 처벌하고 있으며, 여기서 '이미지'를 '변경 여부에 관계없이 정지하거나 움직이는 이미지를 의미한다'고 규정하고 있다는 점이 특징이다. 위 법은 이미지에 조작이 가해졌는지 여부에 관계없이 특정인을 나타내며 동의 없이 성적인 개인 이미지를 촬영 또는 유포하는 경

72) 호주법에서 벌칙 단위(약칭 PU)는 법령 위반에 대한 금전적 벌칙을 계산하는 데 사용되는 금액이다. 벌금은 1개의 벌칙 단위의 값에 위반에 대해 규정된 벌칙 단위의 수를 곱하여 계산한다. 2020년 기준 호주 연방의 벌칙단위는 단위당 222호주 달러이다.

우 100벌칙 단위 혹은 3년 이하의 징역에 처해진다(91N, 91P, 91Q). 즉, 특정인의 신체에 다른 개인의 얼굴을 인공지능 등을 사용하여 합성 제작하였더라도 얼굴이 드러난 자에 대하여 범죄를 저지르는 행위에 해당할 수 있다.⁷³⁾

91N Definitions

(1) In this Division—

distribute includes—

- (a) send, supply, exhibit, transmit or communicate to another person, or
- (b) make available for viewing or access by another person, whether in person or by electronic, digital or any other means.

engaged in a private act means—

- (a) in a state of undress, or
- (b) using the toilet, showering or bathing, or
- (c) engaged in a sexual act of a kind not ordinarily done in public, or
- (d) engaged in any other like activity.

image means a still or moving image, whether or not altered.

intimate image means—

- (a) an image of a person's private parts, or of a person engaged in a private act, in circumstances in which a reasonable person would reasonably expect to be afforded privacy, or
- (b) an image that has been altered to appear to show a person's private parts, or a person engaged in a private act, in circumstances in which a reasonable person w

73) 「Legal Guide to Image-Based Abuse Legislation in NSW」, Australia's NGO Expert on Technology and Violence Against Women 참고.(링크 : https://techsafety.org.au/blog/legal_articles/legal-guide-to-image-based-abuse-legislation-in-nsw/?_cf_chl_jschl_tk__=94f279d7eb7d3cfed0023e61964dac842068c97e-1596106608-0-A_YbOs3spC1PYqTcDKVP8wrmuZOJR62LsSc7a_uLvnqbsEn7HWNVUSGJR3rBvuXjKoxNDK2z6xFG7wvvyuM6sdpCujVHumLNNvZudQLJqYwpZ75n9gWnmj3hf4JoyumZdjYwk-Drhvv5yJw1neIduGHbENXMXrNlepYl6i0MbWAALE3mc5FabyICvJct13CSNBKQuvWrcZgop9WlFTsnGhoB3gIXoq9wNtxeYX6IX8QzTB8IaQwdXQfqS9ZbPIFA3irt20Al_mVyKiG9sUOtj48Q9v0z_gLNxwN_Kkr0RGhGWB89VhGG7nzYbiAC_MwoJ-tNWsgoL_RqtZhDoYmvVxiEV9uwVtnDbHQvSGdIQkm5vlRh2kAehQ_0mZAQGHOVNtjYAOdoti2VtqGsM3D8ZYg_Wql3KzEyp1fxQOseWwcAhAbIzkbYY8uNv0Od7oLIQ)

ould reasonably expect to be afforded privacy.

private parts means—

- (a) a person's genital area or anal area, whether bare or covered by underwear, or
- (b) the breasts of a female person, or transgender or intersex person identifying as female, whether or not the breasts are sexually developed.

91P Record intimate image without consent

(1) A person who intentionally records an intimate image of another person—

- (a) without the consent of the person, and
 - (b) knowing the person did not consent to the recording or being reckless as to whether the person consented to the recording,
- is guilty of an offence.

Maximum penalty—100 penalty units or imprisonment for 3 years, or both.

91Q Distribute intimate image without consent

(1) A person who intentionally distributes an intimate image of another person—

- (a) without the consent of the person, and
 - (b) knowing the person did not consent to the distribution or being reckless as to whether the person consented to the distribution,
- is guilty of an offence.

Maximum penalty—100 penalty units or imprisonment for 3 years, or both.

또한 법원은 위 각 범죄행위에 해당하는 경우 당사자에게 법원이 지정한 기간 내에 당사자가 촬영했거나 유포한 개인적 이미지는 제거, 철회, 복구, 삭제 또는 파기하기 위한 합리적 조치를 취할 것을 명령할 수 있으며(91S-(1)), 합리적 이유 없이 위 명령을 위반하는 경우 50처벌 단위 혹은 2년 이하의 징역에 처할 수 있다(91S-(2)).

91S Court may order rectification

(1) A court that finds a person guilty of an offence against section 91P or 91Q may order the person to take reasonable actions to remove, retract, recover, delete or destroy any intimate image recorded or distributed by the person in contravention of the section within a period specified by the court.

(2) A person who, without reasonable excuse, contravenes an order made under this

section is guilty of an offence.

Maximum penalty—50 penalty units or imprisonment for 2 years, or both.

5. 중국

중국정부는 2019. 12. 딥페이크와 같은 영상 조작에 관한 규제 조항을 포함한 법률 '네트워크 오디오 및 비디오 정보 서비스 관리규정(网络音视频信息服务管理规定, Regulations on the Administration of Network Audio and Video Information Services)'을 제정하여 2020. 1. 1.부터 시행하였다.

위 법은 온라인 오디오·영상정보서비스의 건전하고 질서 있는 발전을 촉진하기 위하여 제정된 것으로, 온라인 오디오·영상정보서비스를 제공하는 자를 그 규율 대상으로 한다. 규율 대상인 '온라인 오디오·영상정보서비스'는 인터넷 사이트 및 응용 프로그램과 같은 네트워크 플랫폼을 통해 일반인에게 오디오 및 비디오 정보를 제작, 배포 및 보급하는 서비스를 의미하며 동영상 등을 게시할 수 있는 플랫폼을 뜻한다(제1조 및 제2조).

위 법은 딥페이크에 관한 정의 조항을 따로 두지는 아니하지만 '리얼 러닝 및 가상 현실을 기반으로 새로운 기술과 응용 프로그램을 사용하여 오디오 및 비디오 정보를 생성'하는 등의 행위 규제하여 실질적으로 딥페이크 기술을 규제한다고 볼 수 있다(제11조). 이에 위 법은 리얼 러닝 및 가상 현실을 기반으로 새로운 기술과 응용 프로그램을 사용하여 오디오 및 비디오 정보를 생성, 게시 및 배포하는 온라인 오디오·영상정보서비스 제공자 및 온라인 오디오·영상정보서비스 사용자는 리얼 러닝 및 가상 현실이라는 점을 표시하여야 한다는 점을 명시하고 있다(제11조).

또한 위 법안은 온라인 오디오·영상정보서비스 제공 업체와 온라인 오디오·영상정보서비스 사용자는 딥 러닝, 가상 현실 등에 기반한 새로운 기술 및 응용 프로그램을 사용하여 허위 뉴스 정보를 작성, 게시 또는 배포해서는 안 된다고 규정하고 있으며,

오디오 및 비디오 뉴스 정보가 생산되는 경우 주(state)가 정한 범위 내에서의 단위로 발행 된 오디오 및 비디오 뉴스 정보는 법률에 부합하여야 함을 명시한다(제11조).

第一条 为促进网络音视频信息服务健康有序发展,保护公民、法人和其他组织的合法权益,维护国家安全和公共利益,根据《中华人民共和国网络安全法》《互联网信息服务管理办法》《互联网新闻信息服务管理规定》《互联网文化管理暂行规定》《互联网视听节目服务管理规定》,制定本规定。

第二条 在中华人民共和国境内从事网络音视频信息服务,应当遵守本规定。
本规定所称网络音视频信息服务,是指通过互联网站、应用程序等网络平台,向社会公众提供音视频信息制作、发布、传播的服务。
网络音视频信息服务提供者,是指向社会公众提供网络音视频信息服务的组织或者个人。
网络音视频信息服务使用者,是指使用网络音视频信息服务的组织或者个人。

第十一条 网络音视频信息服务提供者和网络音视频信息服务使用者利用基于深度学习、虚拟现实等新技术新应用制作、发布、传播非真实音视频信息的,应当以显著方式予以标识。
网络音视频信息服务提供者和网络音视频信息服务使用者不得利用基于深度学习、虚拟现实等新技术新应用制作、发布、传播虚假新闻信息。转载音视频新闻信息的,应当依法转载国家规定范围内的单位发布的音视频新闻信息。

또한 위 법은 사이버 보안, 문화 및 관광, 라디오 및 텔레비전과 관련된 부서에게 각자의 분야에 따른 온라인 오디오·영상정보서비스에 대한 관리감독 의무를 부과하고 있으며(제3조), 이에 더하여 국가가 온라인 오디오·영상정보서비스에 대한 산업 표준 지침 등을 수립 및 개선하며 건전한 산업 시스템을 구축할 것을 선언하고 있다(제4조).

第三条 各级网信、文化和旅游、广播电视等部门依据各自职责开展网络音视频信息服务的监督管理工作。

第四条 网络音视频信息服务提供者 and 使用者应当遵守宪法、法律和行政法规,坚持正确政治方向、舆论导向和价值取向,弘扬社会主义核心价值观,促进形成积极健康、向上向善

的网络文化。

위 법은 온라인 오디오·영상정보서비스 제공자에게 정보보안관리에 대한 일반적인 감독 의무와 전문가를 임명하여 보안사고 및 불법, 범죄 행위를 방지할 의무를 부과한다(제7조). 이에 더하여 온라인 오디오·영상정보서비스 제공자는 딥 러닝 및 가상 현실과 같은 새로운 기술 및 새로운 응용 프로그램에 기초한 오디오 및 비디오 정보 서비스를 시작하거나 관련 기능을 조정 및 추가하는 경우 관련 국가 규정에 따른 보안평가를 수행해야 한다(제10조).

第七条 网络音视频信息服务提供者应当落实信息内容安全管理主体责任，配备与服务规模相适应的专业人员，建立健全用户注册、信息发布审核、信息安全管理、应急处置、从业人员教育培训、未成年人保护、知识产权保护等制度，具有与新技术新应用发展相适应的安全可控的技术保障和防范措施，有效应对网络安全事件，防范网络违法犯罪活动，维护网络数据的完整性、安全性和可用性。

第十条 网络音视频信息服务提供者基于深度学习、虚拟现实等新技术新应用上线具有媒体属性或者社会动员功能的音视频信息服务，或者调整增设相关功能的，应当按照国家有关规定开展安全评估。

위 법은 온라인 오디오·영상정보서비스 제공자로 하여금 오디오 및 비디오 정보 관리를 강화하고 불법, 그리고 가상 오디오 및 비디오 식별 기술을 배치 및 적용하여 이를 발견할 의무를 부과한다(제12조). 온라인 오디오·영상정보서비스 제공자는 오디오 및 비디오 정보 서비스 사용자가 법률 및 규정에 의해 금지된 정보를 생성, 게시 및 유포하는 경우 법률에 따라 정보의 전송을 중지하여 정보의 확산을 방지하고 삭제 등과 같은 조치를 취해야 한다(제12조). 또한 이러한 점을 인터넷 정보, 문화 및 관광, 라디오 및 텔레비전을 관리하는 각 부서에 보고할 의무를 진다(제12조). 이에 더하여 온라인 오디오·영상정보서비스 제공자는 정보 콘텐츠가 본 규정 제11조 제1항의 요구 사항을 충족하지 않는 것으로 판명되면 즉시 정보 전송을 중단할 수 있으며, 가상이라는 점을 표시하여 전송할 수 있다(제12조).

第十二条 网络音视频信息服务提供者应当加强对网络音视频信息服务使用者发布的音视频信息的管理，部署应用违法违规音视频以及非真实音视频鉴别技术，发现音视频信息服务使用者制作、发布、传播法律法规禁止的信息内容的，应当依法依约停止传输该信息，采取消除等处置措施，防止信息扩散，保存有关记录，并向网信、文化和旅游、广播电视等部门报告。

网络音视频信息服务提供者发现不符合本规定第十一条第一款要求的信息内容的，应当立即停止传输该信息，以显著方式标识后方可继续传输该信息。

또한 위 법은 온라인 오디오·영상정보서비스 제공자로 하여금 허위사실 거부 메커니즘(rumor rejection mechanism)을 수립·개선하고, 온라인 오디오·영상정보 서비스 이용자가 딥러닝·가상현실 등에 기반한 허위 이미지를 사용하여 루머를 제작·게시·확산·확산하는 것을 발견하여야 한다는 점을 명시한다(제13조). 온라인 오디오·영상정보서비스 제공자는 적기에 허위사실(rumor) 불식시킬 수 있는 적절한 조치를 취하고, 관련 정보를 인터넷, 문화관광, 라디오, 텔레비전 부서에 보고하여 기록을 남겨야 한다(제13조).

第十三条 网络音视频信息服务提供者应当建立健全辟谣机制，发现网络音视频信息服务使用者利用基于深度学习、虚拟现实等的虚假图像、音视频生成技术制作、发布、传播谣言的，应当及时采取相应的辟谣措施，并将相关信息报网信、文化和旅游、广播电视等部门备案。

네트워크 오디오·영상정보 서비스 이용자에 대하여는 이 규정과 관련 법규를 준수하도록 요구하며 위반한 온라인 오디오·영상정보 서비스 이용자에 대해서는 서비스 제공자가 경고 시정, 기능 제한, 법률에 따른 업데이트 중지, 계정 폐쇄 및 기타 폐기 조치, 관련 기록 저장 등을 할 수 있고, 서비스 제공자가 인터넷·문화관광 담당자에게 보고하도록 하고 있다(제14조).

第十四条 网络音视频信息服务提供者应当在与网络音视频信息服务使用者签订的服务协议

中, 明确双方权利、义务, 要求网络音视频信息服务使用者遵守本规定及相关法律法规。对违反本规定、相关法律法规及服务协议的网路音视频信息服务使用者依法依约采取警示整改、限制功能、暂停更新、关闭账号等处置措施, 保存有关记录, 并向网信、文化和旅游、广播电视等部门报告。

온라인 오디오·영상정보제공자와 이용자가 이 규정을 위반할 경우, 네트워크 정보·문화관광·라디오·텔레비전 부서는 '중화인민공화국 네트워크 보안법' 및 '인터넷 정보 서비스 관리법'을 준수하여야 하고 '인터넷뉴스정보서비스 관리규정', '인터넷문화관리 중간규정', '인터넷시청각프로그램 서비스관리규정' 및 그 밖의 관련 법규에 따라 처리할 것이며, 보안관리 위반이 성립될 때에는 공안관리과징금을 부과하고, 위반행위에 관하여는 형사 책임을 진다(제18조).

第十八条 网络音视频信息服务提供者和网络音视频信息服务使用者违反本规定的, 由网信、文化和旅游、广播电视等部门依照《中华人民共和国网络安全法》《互联网信息服务管理办法》《互联网新闻信息服务管理规定》《互联网文化管理暂行规定》《互联网视听节目服务管理规定》等相关法律法规规定处理; 构成违反治安管理行为的, 依法给予治安管理处罚; 构成犯罪的, 依法追究刑事责任。

위 '중화인민공화국 네트워크 보안법' 제21조는 네트워크 사업자로 하여금 기타 법률 및 행정규정에 규정된 의무를 수행하도록 정하며, 동법 제59조는 네트워크 운영자가 위 조항을 위반하였을시 1만에서 10만 위안의 벌금이 부과되며 직접 책임자에게는 5천에서 5만 위안의 벌금이 부과된다고 정하고 있다.

中华人民共和国网络安全法

第二十一条 国家实行网络安全等级保护制度。网络运营者应当按照网络安全等级保护制度的要求, 履行下列安全保护义务, 保障网络免受干扰、破坏或者未经授权的访问, 防止网络数据泄露或者被窃取、篡改:

- (一) 制定内部安全管理制度和操作规程, 确定网络安全负责人, 落实网络安全保护责任;
- (二) 采取防范计算机病毒和网络攻击、网络侵入等危害网络安全行为的技术措施;
- (三) 采取监测、记录网络运行状态、网络安全事件的技术措施, 并按照规定留存相

의 네트워크 로그는 6개월 이상;

(四) 데이터 분류, 중요 데이터 백업 및 암호화 조치;

(五) 법률, 행정법규规定的其他义务。

第五十九条网络运营者不履行本法第二十一条、第二十五条规定的网络安全保护义务的, 由有关主管部门责令改正, 给予警告; 拒不改正或者导致危害网络安全等后果的, 处一万元以上十万元以下罚款, 对直接负责的主管人员处五千元以上五万元以下罚款。

关键信息基础设施的运营者不履行本法第三十三条、第三十四条、第三十六条、第三十八条规定的网络安全保护义务的, 由有关主管部门责令改正, 给予警告; 拒不改正或者导致危害网络安全等后果的, 处十万元以上一百万元以下罚款, 对直接负责的主管人员处一万元以上十万元以下罚款。

‘인터넷 정보서비스 관리법’은 특정 사업장 또는 개인이 법률 및 행정 규정에서 금지하는 기타 콘텐츠를 포함하는 내용의 정보를 생산, 재생산, 출판 또는 유포하거나 해당 내용을 포함하는 정보의 생산, 복제, 공개 또는 보급을 위한 서비스를 제공할 수 없다고 규정하며, 인터넷 접속 서비스 제공자가 이를 위반하는 경우 관할 부서 및 공안 기관은 해당 불법 행위 중단 명령을 내리고 제공자가 불법적 이익을 얻은 경우에는 해당 불법 소득을 몰수하고 소득의 3-5배의 벌금을 부과하도록 규정하고 있다.

또한 '인터넷뉴스정보서비스 관리규정' 제16조는 인터넷 뉴스 정보 서비스 제공자는 법령에서 금지하는 콘텐츠의 제작, 복사, 게시 및 유포를 하면 안 된다는 의무를 규정하여 동 규정 제24조는 제16조 위반시 유관부서의 시정명령에 응하지 않으면 5천에서 3만 위안의 과태료를 부과한다고 정하고 있다.

互联网信息服务管理办法

第十八条 任何单位和个人不得制作、复制、发布、传播含有下列内容的信息, 或者故意为制作、复制、发布、传播含有下列内容的信息提供服务:

(一) 反对宪法所确定的基本原则的;

(二) 危害国家安全, 泄露国家秘密, 颠覆国家政权, 破坏国家统一的;

(三) 损害国家荣誉和利益的;

(四) 煽动民族仇恨、民族歧视, 破坏民族团结的;

- (五)破坏国家宗教政策，宣扬邪教和封建迷信的；
- (六)散布谣言，煽动非法聚集，扰乱社会秩序，破坏社会稳定的；
- (七)散布淫秽、色情、赌博、暴力、凶杀、恐怖或者教唆犯罪，或者交易、制造违禁品、管制物品的；
- (八)侮辱或者诽谤他人，侵害他人合法权益的，或者仿冒、假借国家机构、社会团体或其他法人名义的；
- (九)含有法律、行政法规禁止的其他内容的。

第三十三条 互联网接入服务提供者违反本办法第十一条、第十四条、第十五条规定的，由电信主管部门给予警告，责令限期改正，并处10万元以上100万元以下罚款；情节严重的，吊销其电信业务经营许可证。

互联网接入服务提供者违反本办法第十六条、第十九条规定的，由电信主管部门、公安机关依照职责给予警告，责令限期改正；逾期未改正的，由电信主管部门处10万元以上100万元以下罚款；情节严重的，吊销其电信业务经营许可证。

互联网接入服务提供者违反本办法第十八条规定，故意为制作、复制、发布、传播违法信息提供服务的，由电信主管部门、公安机关依照职责责令停止违法活动；有违法所得的，由电信主管部门没收违法所得，处违法所得3倍以上5倍以下罚款；情节严重的，吊销其电信业务经营许可证。

6. 일본

현재 일본은 딥페이크 자체를 규제하는 법안이 존재하지 않으며 관련 규제를 입법화하기 위해 논의 중이다(nhk 2020. 4. 8.자 기사⁷⁴⁾).

다만 일본은 개인의 성적 이미지 등을 유포하는 경우 '사사로운 성적 이미지 기록의 제공 등에 의한 피해의 방지에 관한 법률(私事性的画像記録の提供等による被害の防止に関する法律, Act on Prevention of Damage by Providing Private Sexual Image Recording)'을 통해 규제하고 있다. 위 법은 제3자가 촬영대상자를 특정할 수 있는 방법으로 전기통신회선을 통하여 개인의 성적 화상기록을 불특정 또는 다수의 사람에게 제공한 자, 그리고 위의 방법으로 기록물을 불특정 또는 다수에게 공공연하게 진열한

74) <https://www.nhk.or.jp/kokusaihoudou/archive/2020/04/0408.html>

자를 3년 이하의 징역 또는 오십만원 이하의 벌금에 처하도록 규정한다(제3조 제1항, 제2항).

私事性的画像記録の提供等による被害の防止に関する法律

第三条 第三者が撮影対象者を特定することができる方法で、電気通信回線を通じて私事性的画像記録を不特定又は多数の者に提供した者は、三年以下の懲役又は五十万円以下の罰金に処する。

2 前項の方法で、私事性的画像記録物を不特定若しくは多数の者に提供し、又は公然と陳列した者も、同項と同様とする。

또한 위 행위를 하게 할 목적으로 전기통신 회선을 통하여 개인의 성적 화상기록을 제공하거나 개인의 성적 화상기록물을 제공한 자 역시 1년 이하의 징역 또는 삼십만원 이하의 벌금에 처하도록 규정하고 있다(제3조 제3항).

私事性的画像記録の提供等による被害の防止に関する法律

第三条

3 前二項の行為をさせる目的で、電気通信回線を通じて私事性的画像記録を提供し、又は私事性的画像記録物を提供した者は、一年以下の懲役又は三十万円以下の罰金に処する。

위 '개인의 성적 화상기록'이란 (1) 성교 또는 성교 유사행위와 관련된 사람의 자태
2) 타인이 사람의 성기 등(성기, 항문 또는 젖꼭지를 말한다. 이하 본 호 및 다음 호에서도 동일)를 만지는 행위 또는 사람이 타인의 성기 등을 만지는 행위와 관련된 사람의 자태로서 성욕을 흥분시키거나 자극하는 것 (3) 의복의 전부 또는 일부를 착용하지 않은 사람의 자태로서, 특히 사람의 성적인 부위(성기 등이나 그 주변부, 엉덩이 부분 또는 홍부를 말한다.)가 노출되거나 강조되어 있는 것이며, 성욕을 흥분시키거나 자극하는 것 중 등장하는 자의 동의를 받지 아니한 촬영물을 의미한다(제2조).

私事性的画像記録の提供等による被害の防止に関する法律

第二条 この法律において「私事性的画像記録」とは、次の各号のいずれかに掲げる人の姿態が撮影された画像（撮影の対象とされた者（以下「撮影対象者」という。）において、撮影をした者、撮影対象者及び撮影対象者から提供を受けた者以外の者（次条第一項において「第三者」という。）が閲覧することを認識した上で、任意に撮影を承諾し又は撮影をしたものを除く。次項において同じ。）に係る電磁的記録（電子的方式、磁気的方式その他人の知覚によっては認識することができない方式で作られる記録であって、電子計算機による情報処理の用に供されるものをいう。同項において同じ。）その他の記録をいう。

一 性交又は性交類似行為に係る人の姿態

二 他人が人の性器等（性器、肛こう門又は乳首をいう。以下この号及び次号において同じ。）を触る行為又は人が他人の性器等を触る行為に係る人の姿態であって性欲を興奮させ又は刺激するもの

三 衣服の全部又は一部を着けない人の姿態であって、殊更に人の性的な部位（性器等若しくはその周辺部、臀でん部又は胸部をいう。）が露出され又は強調されているものであり、かつ、性欲を興奮させ又は刺激するもの

2 この法律において「私事性的画像記録物」とは、写真、電磁的記録に係る記録媒体その他の物であって、前項各号のいずれかに掲げる人の姿態が撮影された画像を記録したものをいう。

다만 앞서 설명한 바와 같이, 위 촬영물은 실제 사람을 촬영한 경우를 의미하여 딥페이크 기술이 사용된 이미지에까지 적용되는지는 명확하지 않으며 딥페이크 기술을 사용하여 생성된 이미지의 유포 등에 직접 적용되는 법률은 존재하지 않는다. 따라서 현재 일본 당국은 문제를 인식하고 입법과정을 추진하는 중이다.

7. 결어

위에서 살펴본 바와 같이 딥페이크에 관하여 독립된 법안을 다루고 있는 것은 미국이 유일하다. 미국의 연방차원에서 입법 추진되고 있는 법안이 상당히 구체적이거나 아직 본격적으로 시행되지는 않고 있다. 미국은 연방차원의 법안 이외의 각 주에서도 딥페이크를 음란물, 프라이버시, 명예훼손, 개인정보, 플랫폼 사업자의 책임, 선거, 가짜뉴스 등 여러 주제에서 접근하여 법을 마련하거나 입법이 추진되고 있다.

그 이외의 국가들은 딥페이크에 대하여 정면으로 다룬 독립된 법안을 가지고 있지 아니하며, 각 국이 주로 관심을 가지고 있는 이슈에 맞게 추가적인 입법이 추진되었다.

EU는 허위조작정보의 측면에서 권고적인 규약을 발표하였고, 프랑스는 선거, 가짜 뉴스에 초점을 두어 허위조작정보를 규제하는 법안을 시행 중이다. 독일은 일정규모 이상의 소셜네트워크 운영자에게 위법한 콘텐츠에 대한 조치를 취할 의무를 부과하는 형식으로 규제하고 있다.

호주의 경우 음란물의 관점에서 온라인영상을 규제하고 있으며, 중국은 더욱 포괄적인 영상조작의 관점에서 접근하고 있다. 일본은 아직 딥페이크를 다루기 위한 새로운 입법이 추진된 것이 없으며 기존에 존재하는 음란물 관련 법령을 통해 딥페이크 영상을 규제할 수 있다.

이하에서는 해외 기술 및 입법 동향에서 살펴본 내용을 기초로 하여 국내 입법 및 제도 현황에 대하여 검토하도록 한다.

제3장 딥페이크 기술 관련 국내 입법 현황 및 개선논의

제1절 서설

딥페이크 기술은 음란물, 명예훼손, 퍼블리시티권, 초상권 침해, 저작권, 보이스피싱, 피해자의 삭제, 처리정지 등 조치요구, 정보통신서비스 제공자의 의무와 책임, 선거 등 법적이슈와 관련되어 있다.

해외에서는 딥페이크 기술 관련하여 종합적인 단독 법률안이 발의된 것은 미국이 유일하나, 현재 입법 진행 중이며 본격적으로 시행되고 있는 법률은 없다. 그 외 미국 각주, EU, 프랑스, 독일 등에서는 딥페이크를 단독적으로 다루기보다는 음란물, 선거, 허위정보 등 상위개념 관점에서 접근하고 있으며, 플랫폼 운영자의 의무와 책임에 대해서도 상당한 입법이 진행되었다.

국내에서는 아직 딥페이크 관련 단독 법률안이 발의된 것은 없고, 딥페이크 관련 쟁점 별로 개별 법령에 대한 개정이 진행되고 있다.

국내에서 딥페이크 관련하여 가장 발빠르게 입법이 이루어진 영역은 바로 '음란물'로서, 2020. 3. 24. 성폭력범죄의 처벌 등에 관한 특례법(이하 '성폭력처벌법') 제14조의2가 신설되어 2020. 6. 25.부터 시행되고 있다. 성폭력처벌법 제14조의2는 딥페이크 기술로 생성된 영상을 대상자의 의사에 반하여 편집·합성 또는 가공하거나, 반포한 경우를 처벌하고 있으며, 영리목적으로 한 경우 또는 상습으로 한 경우에는 가중 처벌한다.

최근에는 정보통신망 이용촉진 및 정보보호 등에 관한 법률(이하 '정보통신망법') 일부개정법률안이 발의되었으며, 위 개정법률안은 2020. 6. 29. 공포되어 2020. 12. 10.부터 시행예정이다. 개정된 정보통신망법에서는 과학기술정보통신부장관 또는 방송통신위원회로 하여금 딥페이크 관련 기술에 관한 시책을 마련하도록 하였고(정보통신망

법 제4조 제2항 7의2호), 일정규모 이상의 정보통신서비스 제공자로 하여금 딥페이크 기술로 생성된 음란물의 유통을 방지하기 위한 책임자를 지정하고(동법 제44조의 9), 불법촬영물 등의 유통방지와 관련된 각종 사항에 대한 보고서 작성 및 제출 의무를 부여하였다(동법 제64조의5).

그 외에 현재 2020. 8. 6. 권인숙의원 등 11인이 성폭력처벌법 일부개정법률안을 발의하였는데, 위 일부개정법률안은 딥페이크 음란물 피해자의 구제 및 보호 차원에서 피해자와 그 가족이 사생활보호 등의 사유로 불법촬영물과 관련된 증거물의 비공개를 신청할 수 있도록 하는 내용을 담고 있다.

위와 같이 국내 딥페이크 관련 입법은 주로 음란물 규제, 플랫폼 운영자의 책임과 의무, 정부의 시책마련 등의 분야에서 이루어지고 있다.

이하에서는 딥페이크 기술과 관련된 법적이슈와 관련 국내 입법현황을 살펴보고, 기존 법령의 내용을 분석하여 입법적으로 개선되어야 할 사항이 있는지에 관하여 검토하도록 한다.

제2절 딥페이크 관련 법적이슈와 국내 입법 현황

1. 음란물

가. 서설

딥페이크 기술과 관련하여 가장 악질적으로 역기능이 나타나고 있는 분야는 단연 음란물이다. 딥페이크 기술은 다른 사람이 촬영한 음란물에 유명인의 얼굴만을 덧입힘으로써, 마치 유명인이 실제 음란물을 촬영한 것과 같은 효과를 만들어낸다. 딥페이크를 이용한 음란물은 주로 유명 여자아이돌, 배우 등을 타겟으로 하여 제작되고 있다. 얼마 전 국내 연예인 100여 명의 얼굴을 음란물에 합성한 딥페이크 영상 유포자에 대한 본격적인 수사가 개시되었다는 보도가 있었다⁷⁵⁾. 최근에는 모바일 어플리케이션에도 딥페이크 기술이 탑재되어 일반인도 손쉽게 딥페이크 영상을 제작할 수 있는 여건이 조성되었는데, 유명인이 아닌 일반인도 의 피해자가 될 수 있는 가능성이 높아졌다.

나. 성폭력범죄의 처벌 등에 관한 특례법

위와 같이 딥페이크 기술을 이용한 음란물에 대한 형사처벌 조항이 절실한바, 다행히 2020. 3. 24. 딥페이크 기술에 관한 처벌규정이 성폭력범죄의 처벌 등에 관한 특례법(이하 '성폭력처벌법') 제14조의 2로 신설되었다.

성폭력처벌법 제14조의2 제1항은 반포등(반포·판매·임대·제공 또는 공공연하게 전시·상영⁷⁶⁾)의 목적으로 사람의 얼굴·신체 또는 음성을 대상으로 한 촬영물·영상물

75) 2020. 4. 21.자 이데일리 기사 - '女연예인 얼굴 합성' 딥페이크 음란물 유포.. 수사 中
<https://www.edaily.co.kr/news/read?newsId=01498966625738416&mediaCodeNo=257&OutLnkChk=Y>

76) 성폭력처벌법 제14조 제2항의 '반포 등' 정의에 의한다.

또는 음성물(이하 이 조에서 "영상물등"이라 한다)을 영상물등의 대상자의 의사에 반하여 성적 욕망 또는 수치심을 유발할 수 있는 형태로 편집·합성 또는 가공(이하 이 조에서 "편집등"이라 한다)한 자는 5년 이하의 징역 또는 5천만원 이하의 벌금에 처한다고 규정하고 있다.

위 제1항의 '영상물등의 대상자'가 바로 딥페이크의 대상이 된 인물을 뜻하며, 위 대상자의 의사에 반하여 성적 욕망 또는 수치심을 유발할 수 있는 형태로 편집·합성 또는 가공하는 행위는 딥페이크 영상의 편집을 의미한다.

위와 같이 성폭력처벌법 제14조의2 제1항은 직접적으로 딥페이크라는 용어를 사용하면서 이에 대한 정의를 내리고 있지는 아니하나, 딥페이크를 포함하는 넓은 의미의 허위영상물을 규제하고 있으며, 딥페이크 기술을 이용한 편집행위에 한정하지 아니하고 대상자의 의사에 반하여 성적 욕망 또는 수치심을 유발할 수 있는 형태로의 편집, 합성, 가공 등 일체를 규제하고 있다.

성폭력처벌법 제14조의2 제2항에서는 제1항에 따른 편집물·합성물·가공물(이하 이 항에서 "편집물등"이라 한다) 또는 복제물(복제물의 복제물을 포함한다. 이하 이 항에서 같다)을 반포등 한 자 또는 제1항의 편집등을 할 당시에는 영상물등의 대상자의 의사에 반하지 아니한 경우에도 사후에 그 편집물등 또는 복제물을 영상물등의 대상자의 의사에 반하여 반포등 한 자는 5년 이하의 징역 또는 5천만원 이하의 벌금에 처한다고 규정하고 있다.

성폭력처벌법 제14조의2 제2항은 편집 당시에 대상자의 의사에 반하지 아니한 경우에도 반포 시 대상자의 의사에 반한 경우라면 형사처벌의 대상으로 삼고 있는데, 이는 성폭력처벌법 제14조의2의 참조규정인 동법 제14조 제2항에서 "(제14조) 제1항의 촬영이 촬영 당시에는 촬영대상자의 의사에 반하지 아니한 경우(자신의 신체를 직접 촬영한 경우를 포함한다)에도 사후에 그 촬영물 또는 복제물을 촬영대상자의 의사에 반하여 반포등을 한 자"라고 규정하고 있는 것을 해당 조항에도 그대로 적용한 것이다.

성폭력처벌법 제14조의2 제3항에서는 영리를 목적으로 영상물등의 대상자의 의사에

반하여 정보통신망을 이용하여 제2항의 죄를 범한 자는 7년 이하의 징역에 처한다고 하여 영리목적의 경우 가중처벌하고 있으며, 동조 제4항에서는 상습으로 제1항부터 제3항까지의 죄를 범한 때에는 그 죄에 정한 형의 2분의 1까지 가중라고 하여 상습범 또한 가중처벌 하고 있다. 한편, 동법 제14조의2 신설과 함께 동법 제15조를 개정하여, 제14조의2의 범죄에 대한 미수범 처벌규정도 신설하였다.

성폭력범죄의 처벌 등에 관한 특례법

제14조의2(허위영상물 등의 반포등)

① 반포등을 할 목적으로 사람의 얼굴·신체 또는 음성을 대상으로 한 촬영물·영상물 또는 음성물(이하 이 조에서 "영상물등"이라 한다)을 영상물등의 대상자의 의사에 반하여 성적 욕망 또는 수치심을 유발할 수 있는 형태로 편집·합성 또는 가공(이하 이 조에서 "편집등"이라 한다)한 자는 5년 이하의 징역 또는 5천만원 이하의 벌금에 처한다.

② 제1항에 따른 편집물·합성물·가공물(이하 이 항에서 "편집물등"이라 한다) 또는 복제물(복제물의 복제물을 포함한다. 이하 이 항에서 같다)을 반포등을 한 자 또는 제1항의 편집등을 할 당시에는 영상물등의 대상자의 의사에 반하지 아니한 경우에도 사후에 그 편집물등 또는 복제물을 영상물등의 대상자의 의사에 반하여 반포등을 한 자는 5년 이하의 징역 또는 5천만원 이하의 벌금에 처한다.

③ 영리를 목적으로 영상물등의 대상자의 의사에 반하여 정보통신망을 이용하여 제2항의 죄를 범한 자는 7년 이하의 징역에 처한다.

④ 상습으로 제1항부터 제3항까지의 죄를 범한 때에는 그 죄에 정한 형의 2분의 1까지 가중한다. [신설 2020.5.19] [[시행일 2020.6.25]]

[본조신설 2020.3.24] [[시행일 2020.6.25]]

제15조(미수범)

제3조부터 제9조까지, 제14조 및 제14조의2의 미수범은 처벌한다.

[전문개정 2020.5.19] [[시행일 2020.6.25]]

앞서 언급한 바와 같이, 동법 제14조의2(허위영상물 등의 반포등)은 동법 제14조(카메라 등을 이용한 촬영)을 기본으로 하여 신설된 규정이다. 제14조와 제14조의2의 조문구성을 비교하면 아래와 같다.

<표 3-1> 성폭력처벌법 제14조 및 제14조의2 조문구성 비교

	제14조(카메라 등을 이용한 촬영)	제14조의2(허위영상물 등의 반포등)
제작 등	① 카메라나 그 밖에 이와 유사한 기능을 갖춘 기계장치를 이용하여 성적 욕망 또는 수치심을 유발할 수 있는 사람의 신체를 촬영대상자의 의사에 반하여 촬영한 자는 7년 이하의 징역 또는 5천만원 이하의 벌금에 처한다.	① 반포등을 할 목적으로 사람의 얼굴·신체 또는 음성을 대상으로 한 촬영물·영상물 또는 음성물(이하 이 조에서 "영상물등"이라 한다)을 영상물등의 대상자의 의사에 반하여 성적 욕망 또는 수치심을 유발할 수 있는 형태로 편집·합성 또는 가공(이하 이 조에서 "편집등"이라 한다)한 자는 5년 이하의 징역 또는 5천만원 이하의 벌금에 처한다.
반포 등	② 제1항에 따른 촬영물 또는 복제물(복제물의 복제물을 포함한다. 이하 이 조에서 같다)을 반포·판매·임대·제공 또는 공공연하게 전시·상영(이하 "반포등"이라 한다)한 자 또는 제1항의 촬영이 촬영 당시에는 촬영대상자의 의사에 반하지 아니한 경우(자신의 신체를 직접 촬영한 경우를 포함한다)에도 사후에 그 촬영물 또는 복제물을 촬영대상자의 의사에 반하여 반포등을 한 자는 7년 이하의 징역 또는 5천만원 이하의 벌금에 처한다.	② 제1항에 따른 편집물·합성물·가공물(이하 이 항에서 "편집물등"이라 한다) 또는 복제물(복제물의 복제물을 포함한다. 이하 이 항에서 같다)을 반포등을 한 자 또는 제1항의 편집등을 할 당시에는 영상물등의 대상자의 의사에 반하지 아니한 경우에도 사후에 그 편집물등 또는 복제물을 영상물등의 대상자의 의사에 반하여 반포등을 한 자는 5년 이하의 징역 또는 5천만원 이하의 벌금에 처한다.
영리목적범	③ 영리를 목적으로 촬영대상자의 의사에 반하여 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제2조 제1항제1호의 정보통신망(이하 "정보통신망"이라 한다)을 이용하여 제2항의 죄를 범한 자는 3년 이상의 유기징역에 처한다.	③ 영리를 목적으로 영상물등의 대상자의 의사에 반하여 정보통신망을 이용하여 제2항의 죄를 범한 자는 7년 이하의 징역에 처한다.
상습범	⑤ 상습으로 제1항부터 제3항까지의 죄를 범한 때에는 그 죄에 정한 형의 2분의 1까지 가중한다.	④ 상습으로 제1항부터 제3항까지의 죄를 범한 때에는 그 죄에 정한 형의 2분의 1까지 가중한다.

소 지 법	④ 제1항 또는 제2항의 촬영물 또는 복제물을 <u>소지·구입·저장 또는 시청</u> 한 자는 3년 이하의 징역 또는 3천만원 이하의 벌금에 처한다.	없음
-------------	---	----

위와 같이 제14조의2 제1항은 제14조 제1항과는 달리 영상의 제작 시 반포·판매·임대·제공 또는 공공연하게 전시·상영할 목적을 추가적으로 요구하고 있다. 또한 제14조의2는 제14조에 비하여 형량을 한 단계씩 낮게 규정하고 있으며, 소지·구입·저장 또는 시청의 경우에는 별도로 처벌규정이 없다.

이상의 내용을 종합할 때, 딥페이크 기술로 제작된 허위 음란영상물의 경우 실제 인물을 대상으로 한 비동의 음란물 촬영에 비하여 입법적으로 불법성이 낮게 평가되고 있는 것으로 보인다.

다. 정보통신망 이용촉진 및 정보보호 등에 관한 법률

정보통신망 이용촉진 및 정보보호 등에 관한 법률(이하 '정보통신망법')은 일반적인 음란물 유통에 관한 처벌규정을 두고 있다.

정보통신망법 제44조의7 제1항 제1호는 누구든지 정보통신망을 통하여 부호·문언·음향·화상 또는 영상을 배포·판매·임대하거나 공공연하게 전시하는 내용의 정보를 유통하여서는 아니된다고 규정하고 있으며, 동법 제44조의7 제1항 제1호를 위반하는 경우 동법 제74조 제1항 제2호에 의하여 1년 이하의 징역 또는 1천만원 이하의 벌금으로 처벌된다.

정보통신망(인터넷, SNS, 포털사이트, 어플리케이션 등)을 통하여 딥페이크 기술을 이용하여 제작된 음란한 음향, 화상 또는 영상을 배포·판매·임대하거나 공공연하게 전시하는 경우 형사처벌의 대상이 된다.

정보통신망법
제44조의7(불법정보의 유통금지 등)

① 누구든지 정보통신망을 통하여 다음 각 호의 어느 하나에 해당하는 정보를 유통하여서는 아니 된다.

1. 음란한 부호·문언·음향·화상 또는 영상을 배포·판매·임대하거나 공공연하게 전시하는 내용의 정보

제74조(벌칙)

① 다음 각 호의 어느 하나에 해당하는 자는 1년 이하의 징역 또는 1천만원 이하의 벌금에 처한다.

2. 제44조의7제1항제1호를 위반하여 음란한 부호·문언·음향·화상 또는 영상을 배포·판매·임대하거나 공공연하게 전시한 자

라. 소결

위에서 본 바와 같이, 딥페이크 기술로 생성된 음란물의 유통에 관하여 기존 정보통신망법으로도 규제가 가능하며(제44조의7 제1항 제1호, 제44조의7 제1항 제1호), 딥페이크 기술로 인한 허위 음란영상물의 편집·합성 또는 가공, 반포·판매·임대·제공 또는 공공연하게 전시·상영에 대해서는 최근 성폭력처벌법 제14조의2의 신설로 강력한 처벌규정을 마련하였는바, 딥페이크 기술을 이용한 음란물 제작과 유통을 모두 처벌하고 있어 입법공백이 없는 상태로 보인다.

다만, 성폭력처벌법 제14조의2 제1항은 반포등의 목적없이 제작된 딥페이크 영상의 경우 처벌이 어려운 문제점이 있어 목적조항의 삭제여부를 검토할 필요성이 있으며, 동법 제14조와는 달리 허위 음란영상물을 반포하지 아니하고 소지만한 경우에 대하여는 처벌규정이 없어 이에 대한 규정신설을 검토하여야 한다.

2. 명예훼손·사자명예훼손

가. 서설

딥페이크 기술은 딥페이크의 대상이 된 인물이 실제 행동이나 말을 하지 않았음에도 불구하고, 그러한 행동이나 말을 한 것과 같은 오해를 일으키는 영상을 만들어낼

수 있다.

명예훼손은 진실사실의 적시와 허위사실의 적시를 나누어 허위사실 적시의 경우 가 중처벌하고 있는데, 딥페이크 영상은 하지 않은 행동이나 말을 실제처럼 구현해낼 수 있으므로 특히 허위사실 적시로 인한 명예훼손이 문제될 수 있다.

나. 형법

딥페이크 영상을 이용하여 명예를 훼손한 경우, 진실사실 적시인 경우 2년 이하의 징역이나 금고 또는 500만원 이하의 벌금, 허위사실 적시인 경우 5년 이하의 징역, 10년 이하의 자격정지 또는 1천만원 이하의 벌금에 처해진다.

신문, 잡지, 라디오 기타 출판물 등에 의하여 진실사실을 적시한 경우에는 3년 이하의 징역이나 금고 또는 700만원 이하의 벌금에, 허위사실을 적시한 경우에는 3년 이하의 징역이나 금고 또는 700만원 이하의 벌금에 처해진다.

또한 딥페이크 영상은 살아있는 사람이 아닌 '사망한자'를 대상으로도 제작될 수 있다. 딥페이크 영상이 사망한자를 대상으로 제작되었으며, 그 영상이 허위사실을 적시하여 사망한자의 명예가 훼손되었을 경우 2년 이하의 징역이나 금고 또는 500만원 이하의 벌금에 처해진다.

형법

제307조(명예훼손)

- ① 공연히 사실을 적시하여 사람의 명예를 훼손한 자는 2년 이하의 징역이나 금고 또는 500만원 이하의 벌금에 처한다.
- ② 공연히 허위의 사실을 적시하여 사람의 명예를 훼손한 자는 5년 이하의 징역, 10년 이하의 자격정지 또는 1천만원 이하의 벌금에 처한다.

제308조(사자의 명예훼손)

공연히 허위의 사실을 적시하여 사자의 명예를 훼손한 자는 2년 이하의 징역이나 금고 또는 500만원 이하의 벌금에 처한다.

제309조(출판물등에 의한 명예훼손)

- ① 사람을 비방할 목적으로 신문, 잡지 또는 라디오 기타 출판물에 의하여 제307조제

1항의 죄를 범한 자는 3년 이하의 징역이나 금고 또는 700만원 이하의 벌금에 처한다.

② 제1항의 방법으로 제307조제2항의 죄를 범한 자는 7년 이하의 징역, 10년 이하의 자격정지 또는 1천500만원 이하의 벌금에 처한다.

다. 정보통신망 이용촉진 및 정보보호 등에 관한 법률

정보통신망을 통하여 진실이나 허위사실을 적시하여 타인의 명예를 훼손한 경우 진실사실의 경우에는 3년 이하의 징역 또는 3천만원 이하의 벌금, 허위사실인 경우에는 7년 이하의 징역, 10년 이하의 자격정지 또는 5천만원 이하의 벌금에 처해진다.

정보통신망법

제44조의7(불법정보의 유통금지 등)

① 누구든지 정보통신망을 통하여 다음 각 호의 어느 하나에 해당하는 정보를 유통하여서는 아니 된다.

2. 사람을 비방할 목적으로 공공연하게 사실이나 거짓의 사실을 드러내어 타인의 명예를 훼손하는 내용의 정보

제70조(벌칙)

① 사람을 비방할 목적으로 정보통신망을 통하여 공공연하게 사실을 드러내어 다른 사람의 명예를 훼손한 자는 3년 이하의 징역 또는 3천만원 이하의 벌금에 처한다.

② 사람을 비방할 목적으로 정보통신망을 통하여 공공연하게 거짓의 사실을 드러내어 다른 사람의 명예를 훼손한 자는 7년 이하의 징역, 10년 이하의 자격정지 또는 5천만원 이하의 벌금에 처한다.

라. 소결

위에서 본 바와 같이 딥페이크 영상이 진실사실 적시 또는 허위사실 적시로 특정인에 대한 명예를 훼손한 경우 형사처벌의 대상이 된다. 딥페이크 영상으로 인한 명예훼손이 문제되는 경우 형사처벌규정이 존재하므로 입법 공백이 없는 것으로 보인다.

3. 퍼블리시티권 · 초상권 침해

가. 퍼블리시티권

딥페이크 영상이 유명인의 초상 또는 음성을 기초로 하여 제작되고, 이것이 광고, 영화, 뮤직비디오 등 상업적인 영역에서 사용되어 유명인의 경제적인 이익이 침해된 경우 퍼블리시티권 침해가 문제될 수 있다.

퍼블리시티권(Publicity權)이란 성명이나 초상 등 자기동일성이 가지는 경제적 가치를 상업적으로 사용하고 통제할 수 있는 배타적 권리를 의미한다. 퍼블리시티권은 국내 법령 상 규정되어 있는 실정법상의 권리는 아니나, 행복추구권, 인격권, 성명권 등 헌법적 권리로부터 도출되는 권리이며, 재산권적 성격도 가지고 있다.

서울서부지방법원 2010. 4. 21 자 2010카합245 결정

일반적으로 성명이나 초상 등 자기동일성이 가지는 경제적 가치를 상업적으로 사용하고 통제할 수 있는 배타적 권리라고 설명되는 퍼블리시티권은 이를 명시적으로 규정한 실정법이 존재하지는 않으나, 헌법상의 행복추구권과 인격권의 한 내용을 이루는 성명권에는 사회통념상 특정인임을 알 수 있는 방법으로 성명이 함부로 영리에 사용되지 않을 권리가 포함된다고 할 것인 점, 특정인의 성명 등에 관하여 형성된 경제적 가치가 이미 인터넷 게임업 등 관련 영업에서 널리 인정되고 있으므로 이를 침해하는 행위는 그 특정인에 대한 관계에서 민법상의 불법행위를 구성한다고 볼 것인 점등에 비추어 보면, 특정인이 성명이나 초상 등 자기동일성의 상업적 사용에 대하여 배타적으로 지배할 수 있는 권리를 퍼블리시티권으로 파악하기에 충분하므로, 어떤 사람의 성명 전부 또는 일부를 그대로 사용하는 것은 물론 성명 전부 또는 일부를 그대로 사용하지 않더라도 그 사람을 나타낸다고 볼 수 있을 정도로 이를 변형하여 사용하는 경우에도 퍼블리시티권을 침해한 것으로 볼 것이며, 이러한 퍼블리시티권은 인격권, 행복추구권으로부터 파생된 것이기는 하나 재산권적 성격도 가지고 있다.

나. 초상권

딥페이크 영상은 유명인이 아닌 일반인의 초상을 대상으로 하여도 제작이 가능한

바, 이때 초상권침해가 문제될 수 있다.

초상권은 자신의 얼굴 기타 사회통념상 특정인임을 식별할 수 있는 신체적 특징에 관하여 함부로 촬영 또는 그림묘사되거나 공표되지 아니하며 영리적으로 이용당하지 않을 권리를 뜻한다. 이러한 초상권은 헌법 제10조 제1문⁷⁷⁾의 인간의 존엄과 가치, 행복추구권에 의하여 도출되는 헌법적으로 보장되는 권리이다.

대법원 2006. 10. 13 선고 2004다16280 판결

사람은 누구나 자신의 얼굴 기타 사회통념상 특정인임을 식별할 수 있는 신체적 특징에 관하여 함부로 촬영 또는 그림묘사되거나 공표되지 아니하며 영리적으로 이용당하지 않을 권리를 가지는데, 이러한 초상권은 우리 헌법 제10조 제1문에 의하여 헌법적으로 보장되는 권리이다.

살아있는 사람이 아닌 사망한자의 초상권 또한 문제될 수 있다. 참고로, 미국 뉴욕주에서는 사망한자의 초상권이 사용되는 것에 관하여, 시청각 작품에서 음악 작품의 라이브 공연을 위해 사망한 공연자의 digital replica(디지털 복제본)를 사전 동의 없이 사용하는 자는, 그 사용이 대중을 속일 가능성이 있는 경우, 그 손해에 대한 책임을 진다고 규정하고 있다(퍼블리시티권을 확립하고 성적으로 명백한 묘사를 불법적으로 유포하거나 출판하기 위하여 사적 권리를 제공하는 것과 관련한 민권법 개정법⁷⁸⁾ § 50-f. 2. b.).

다. 소결

딥페이크 영상은 개인의 초상을 기초로 제작되는 경우가 많아 퍼블리시티권과 초상

77) 헌법 제10조 모든 국민은 인간으로서의 존엄과 가치를 가지며, 행복을 추구할 권리를 가진다. 국가는 개인이 가지는 불가침의 기본적 인권을 확인하고 이를 보장할 의무를 진다.

78) An act to amend the civil rights law, in relation to establishing the right of publicity and to providing a private right of action for unlawful dissemination or publication of a sexually explicit depiction of an individual

권이 필연적으로 결부되어 있을 수 밖에 없다.

딤페이크 영상으로 인해 퍼블리시티권 또는 초상권이 침해당한 경우, 피해자는 딤페이크 영상 제작자 또는 유통자에 대하여 경제적인 이익 침해 또는 정신적 피해보상을 근거로 민사상 손해배상청구가 가능하다.

또한 퍼블리시티권과 초상권침해 행위가 별도로 법령 상 범죄구성요건을 충족할 경우 해당 조항 위반으로 인한 형사고소 등이 가능하다.

퍼블리시티권과 초상권 침해의 경우 현행법 상 민사 및 형사상 구제절차가 마련되어 있어 기존 법률로도 충분히 해결이 가능한바, 특별한 입법적인 공백이 있지는 않다.

4. 저작권

대부분의 딤페이크 영상은 원본 영상 또는 이미지 속 인물에 대한 동의가 없이 제작되고 있을 뿐만 아니라, 원본 영상 또는 이미지 저작권자에 대한 동의 없이 제작되고 있다.

딤페이크 영상은 원본 영상 또는 이미지를 기초로 하여 새로운 딤페이크 영상을 생성하므로, 동의 없이 원본 영상을 사용하였을 경우 저작권침해의 문제가 있을 수 있다(제136조 제1항 제1호).

딤페이크 영상을 제작할 시 저작자의 동의 없는 이미지, 영상 또는 음성파일을 이용한 경우 저작권법 제136조 제1항 제1호에 따라 5년 이하의 징역 또는 5천만원 이하의 벌금에 처해질 수 있으며, 원본 영상, 이미지, 음성파일에 대한 저작권자는 동의 없이 원본을 이용하여 딤페이크 영상을 무단으로 제작한 자에 대하여 손해배상, 금지청구 등을 청구할 수 있다.

저작권법

제123조(침해의 정지 등 청구)

① 저작권 그 밖에 이 법에 따라 보호되는 권리(제25조·제31조·제75조·제76조·제76조의2·제82조·제83조 및 제83조의2의 규정에 따른 보상을 받을 권리를 제외한다. 이하 이 조에서 같다)를 가진 자는 그 권리를 침해하는 자에 대하여 침해의 정지를 청구할 수 있으며, 그 권리를 침해할 우려가 있는 자에 대하여 침해의 예방 또는 손해배상의 담보를 청구할 수 있다.

② 저작권 그 밖에 이 법에 따라 보호되는 권리를 가진 자는 제1항의 규정에 따른 청구를 하는 경우에 침해행위에 의하여 만들어진 물건의 폐기나 그 밖의 필요한 조치를 청구할 수 있다.

③ 제1항 및 제2항의 경우 또는 이 법에 따른 형사의 기소가 있는 때에는 법원은 원고 또는 고소인의 신청에 따라 담보를 제공하거나 제공하지 아니하게 하고, 임시로 침해행위의 정지 또는 침해행위로 말미암아 만들어진 물건의 압류 그 밖의 필요한 조치를 명할 수 있다.

④ 제3항의 경우에 저작권 그 밖에 이 법에 따라 보호되는 권리의 침해가 없다는 뜻의 판결이 확정된 때에는 신청자는 그 신청으로 인하여 발생한 손해를 배상하여야 한다.

제125조(손해배상의 청구)

① 저작재산권 그 밖에 이 법에 따라 보호되는 권리(저작인격권 및 실연자의 인격권을 제외한다)를 가진 자(이하 "저작재산권자등"이라 한다)가 고의 또는 과실로 권리를 침해한 자에 대하여 그 침해행위에 의하여 자기가 받은 손해의 배상을 청구하는 경우에 그 권리를 침해한 자가 그 침해행위에 의하여 이익을 받은 때에는 그 이익의 액을 저작재산권자등이 받은 손해의 액으로 추정한다.

② 저작재산권자등이 고의 또는 과실로 그 권리를 침해한 자에 대하여 그 침해행위에 의하여 자기가 받은 손해의 배상을 청구하는 경우에 그 권리의 행사로 통상 받을 수 있는 금액에 상당하는 액을 저작재산권자등이 받은 손해의 액으로 하여 그 손해배상을 청구할 수 있다.

제136조(벌칙)

① 다음 각 호의 어느 하나에 해당하는 자는 5년 이하의 징역 또는 5천만원 이하의 벌금에 처하거나 이를 병과할 수 있다.

1. 저작재산권, 그 밖에 이 법에 따라 보호되는 재산적 권리(제93조에 따른 권리는 제외한다)를 복제, 공연, 공중송신, 전시, 배포, 대여, 2차적저작물 작성의 방법으로 침해한 자

최근 일본에서는 딥페이크 영상으로 만든 음란물에 대하여 명예훼손 및 저작권법 위반혐의를 적용하였다⁷⁹⁾.

원본 영상, 이미지, 음성파일을 딥페이크 저작권자가 무단으로 이용하여 딥페이크 영상을 만든 것에 대하여는 저작권법 상 손해배상 및 형사처벌규정이 마련되어 있어 입법적 공백은 없는 상황이다.

5. 보이스피싱

가. 서설

딥페이크 영상 또는 음성을 이용한 보이스피싱으로 인해 딥페이크 영상을 진실한 것으로 믿은 사람들의 재산상 피해가 발생할 수 있다.

나. 전기통신금융사기 피해 방지 및 피해금 환급에 관한 특별법

전기통신금융사기 피해 방지 및 피해금 환급에 관한 특별법(이하 '통신사기피해환급법') 제2조 제2호에서는 "전기통신금융사기"란 「전기통신기본법」 제2조제1호에 따른 전기통신을 이용하여 타인을 기망(欺罔)·공갈(恐喝)함으로써 재산상의 이익을 취하거나 제3자에게 재산상의 이익을 취하게 하는 자금을 송금·이체하도록 하는 행위, 개인정보를 알아내어 자금을 송금·이체하는 행위를 말한다고 규정하고 있다.

이때의 전기통신은 유선·무선·광선 및 기타의 전자적 방식에 의하여 부호·문언·음향 또는 영상을 송신하거나 수신하는 것을 뜻한다(전기통신기본법 제2조 제1호). 딥페이크 영상은 전자적 방식에 의한 음향 또는 영상에 해당하므로 전기통신에 해당한다.

통신사기피해환급법 제15조의2 제1항에서는 전기통신금융사기를 목적으로 다음 각 호의 어느 하나에 해당하는 행위를 한 자는 10년 이하의 징역 또는 1억원 이하의 벌금에 처한다고 규정하면서⁷⁹⁾, 제1호에서 타인으로 하여금 컴퓨터 등 정보처리장치에

79) 2020. 10. 2.자 디지털타임스 기사

http://www.dt.co.kr/contents.html?article_no=2020100202109919607005&ref=naver

정보 또는 명령을 입력하게 하는 행위, 제2호에서 취득한 타인의 정보를 이용하여 컴퓨터 등 정보처리장치에 정보 또는 명령을 입력하는 행위를 규정하고 있다.

인터넷, SNS, 포털사이트, 어플리케이션, 휴대폰 문자메시지, 이메일 등을 통하여 딥페이크 영상 또는 음성을 전송하는 방법으로 타인을 기망 또는 공갈하여 재산상 이익을 취한 경우 10년 이하의 징역 또는 1억원 이하의 벌금에 처해질 수 있다.

전기통신금융사기 피해 방지 및 피해금 환급에 관한 특별법

제2조(정의)

이 법에서 사용하는 용어의 뜻은 다음과 같다.

2. "전기통신금융사기"란 「전기통신기본법」 제2조제1호에 따른 전기통신을 이용하여 타인을 기망(欺罔)·공갈(恐喝)함으로써 재산상의 이익을 취하거나 제3자에게 재산상의 이익을 취하게 하는 다음 각 목의 행위를 말한다. 다만, 재화의 공급 또는 용역의 제공 등을 가장한 행위는 제외하되, 대출의 제공·알선·중개를 가장한 행위는 포함한다.

가. 자금을 송금·이체하도록 하는 행위

나. 개인정보를 알아내어 자금을 송금·이체하는 행위

제15조의2(벌칙)

① 전기통신금융사기를 목적으로 다음 각 호의 어느 하나에 해당하는 행위를 한 자는 10년 이하의 징역 또는 1억원 이하의 벌금에 처한다.

1. 타인으로 하여금 컴퓨터 등 정보처리장치에 정보 또는 명령을 입력하게 하는 행위

2. 취득한 타인의 정보를 이용하여 컴퓨터 등 정보처리장치에 정보 또는 명령을 입력하는 행위

② 제1항의 미수범은 처벌한다.

③ 상습적으로 제1항의 죄를 범한 자는 그 죄에 대하여 정하는 형의 2분의 1까지 가중한다.

전기통신기본법

80) 통신사기피해환급법 제15조의2 제1항이 처벌대상으로 삼고 있는 '통신사기피해환급법 제2조 제2호에서 정한 전기통신금융사기(이하 '전기통신금융사기'라고 한다)를 목적으로 하는 정보 또는 명령의 입력'이란 '타인에 대한 전기통신금융사기 행위에 의하여 자금을 다른 계좌로 송금·이체하는 것을 목적으로 하는 정보 또는 명령의 입력'을 의미한다고 해석된다(대법원 2016. 2. 19 선고 2015도15101 전원합의체 판결).

제2조(정의)

이 법에서 사용하는 용어의 정의는 다음과 같다.

1. "전기통신"이라 함은 유선·무선·광선 및 기타의 전자적 방식에 의하여 부호·문언·음향 또는 영상을 송신하거나 수신하는 것을 말한다.

다. 소결

보이스피싱 범죄 자체가 거짓으로 목소리 등을 흉내 내어 진짜인 것처럼 믿게한 후 경제적인 이익을 취하는 범죄인바, 그러한 영상 또는 음성 조작의 수단으로서 딥페이크 기술이 이용될 수 있다. 딥페이크 영상 또는 음향을 전송하는 방법으로 보이스피싱 범죄를 저지른 경우, 통신사기피해환급법에 의하여 처벌이 가능하다.

딥페이크 기술을 이용하여 조작된 음성 또는 영상을 제작한 후 보이스피싱 범죄를 저지른 경우 처벌규정이 있어 입법적인 공백은 없는 것으로 보인다.

6. 선거

가. 서설

딥페이크 기술을 활용한 영상이 선거에 활용될 경우, 유권자 의사 형성을 방해함으로써 선거 결과를 왜곡시킬 가능성이 있다.

나. 공직선거법

현행 공직선거법에서 딥페이크 활용 허위 영상과 관련하여 적용이 가능할 것으로 판단되는 조항은 제250조 허위사실공표죄 또는 제110조 후보자 등의 비방금지 등 2개이다.

공직선거법 제110조 제1항은 누구든지 선거운동을 위하여 후보자, 배우자 또는 직

계존비속이나 형제자매의 출생지·가족관계·신분·직업·경력등·재산·행위·소속단체, 특정인 또는 특정단체로부터의 지지여부 등에 관하여 허위의 사실을 공표할 수 없으며, 공연히 사실을 적시하여 사생활을 비방할 수 없다고 규정하고 있다.

제110조 제1항 후보자 비방금지의 경우, 제한규정 위반에 대한 형사처벌 조항은 따로 존재하지 않는다.

공직선거법 제250조 제1항은 당선되거나 되게 할 목적으로 연설·방송·신문·통신·잡지·벽보·선전문서 기타의 방법으로 후보자에게 유리하도록 후보자, 후보자의 배우자 또는 직계존비속이나 형제자매의 출생지·가족관계·신분·직업·경력등·재산·행위·소속단체, 특정인 또는 특정단체로부터의 지지여부 등에 관하여 허위의 사실을 공표하거나 공표하게 한 자와 허위의 사실을 게재한 선전문서를 배포할 목적으로 소지한 자는 5년이하의 징역 또는 3천만원이하의 벌금에 처하고 있다.

제250조의 허위사실공표죄는 제1,3항의 경우 5년 이하의 징역 또는 1천만원 이하의 벌금, 제2항의 경우 7년 이하의 징역 또는 5백만원 이상 3천만원 이하의 벌금 등 형사처벌을 규정하고 있다.

공직선거법

제110조(후보자 등의 비방금지)

① 누구든지 선거운동을 위하여 후보자, 배우자 또는 직계존비속이나 형제자매의 출생지·가족관계·신분·직업·경력등·재산·행위·소속단체, 특정인 또는 특정단체로부터의 지지여부 등에 관하여 허위의 사실을 공표할 수 없으며, 공연히 사실을 적시하여 사생활을 비방할 수 없다. 다만, 진실한 사실로서 공공의 이익에 관한 때에는 그러하지 아니하다.

② 누구든지 선거운동을 위하여 정당, 후보자, 후보자의 배우자 또는 직계존비속이나 형제자매와 관련하여 특정 지역·지역인 또는 성별을 공연히 비하·모욕하여서는 아니 된다.

제250조(허위사실공표죄)

① 당선되거나 되게 할 목적으로 연설·방송·신문·통신·잡지·벽보·선전문서 기타의 방법으로 후보자에게 유리하도록 후보자, 후보자의 배우자 또는 직계존비속이나 형제자매의 출생지·가족관계·신분·직업·경력등·재산·행위·소속단체, 특정인 또는 특정단체로부터의 지지여부 등에 관하여 허위의 사실[학력을 게재하는 경우 제64조제1항의 규정

에 의한 방법으로 게재하지 아니한 경우를 포함한다)을 공표하거나 공표하게 한 자와 허위의 사실을 게재한 선전문서를 배포할 목적으로 소지한 자는 5년이하의 징역 또는 3천만원이하의 벌금에 처한다.

② 당선되지 못하게 할 목적으로 연설·방송·신문·통신·잡지·책보·선전문서 기타의 방법으로 후보자에게 불리하도록 후보자, 그의 배우자 또는 직계존·비속이나 형제자매에 관하여 허위의 사실을 공표하거나 공표하게 한 자와 허위의 사실을 게재한 선전문서를 배포할 목적으로 소지한 자는 7년 이하의 징역 또는 500만원 이상 3천만원 이하의 벌금에 처한다.

③ 당내경선과 관련하여 제1항(제64조 제1항의 규정에 따른 방법으로 학력을 게재하지 아니한 경우를 제외한다)에 규정된 행위를 한 자는 3년 이하의 징역 또는 6백만원 이하의 벌금에, 제2항에 규정된 행위를 한 자는 5년 이하의 징역 또는 1천만원 이하의 벌금에 처한다. 이 경우 "후보자" 또는 "후보자(후보자가 되고자 하는 자를 포함한다)"는 "경선후보자"로 본다.

공직선거법 제110조 제1항의 허위사실 공표와 제250조의 허위사실 공표는 그 구성요건이 유사한 것으로 보이지만, 제110조의 경우 '선거운동을 위하여' 허위사실을 공표하는 행위를 금지하는 반면, 250조의 경우 '당선되거나 되게 할 목적' 또는 '당선되지 못하게 할 목적'을 주관적 구성요건요소로 하는 목적범 형태를 띠고 있다는 차이가 있다.

대법원은 공직선거법 제250조 제2항 '허위사실의 공표'의 의미가 문제된 사건에서, "공직선거및선거부정방지법 제250조 제2항의 행위태양인 '공표'라 함은 그 수단이나 방법의 여하를 불문하고 불특정 또는 다수인에게 허위사실을 알리는 것"을 말한다고 그 의미를 구체화한바 있다. 대법원의 해석론에 따르면, 딥페이크 기술 활용 허위 영상을 유포한 행위가 불특정 또는 다수인에게 허위사실을 알리는 것과 동일시할 수 있는 경우에는 공직선거법 제250조 허위사실 공표 행위로 의율할 수 있을 것으로 판단된다.

참고로 공직선거법 위반 여부가 문제된 사안들 가운데 딥페이크 영상 유포와 유사한 사례군으로는 선거운동에 합성사진을 게시하는 사례가 있다. 2020년 제21대 총선 당시 광주시 서구를 예비후보가 여성 장관의 나체사진을 합성한 현수막을 선거사무실 입주 건물 외벽에 게시한 행위에 대하여, 광주시선거관리위원회에서 이를 공직선거법

제7조 제1항 '선량한 풍속 등 사회질서를 해하는 행위'로서 공정경쟁의무에 위반된다고 본 사례가 있다. 위 사례에서는 공직선거법 제7조 위반에 따른 벌칙 조항이 없어 서면 경고 형태의 행정조치가 취해졌다.

공직선거법

제7조(정당·후보자 등의 공정경쟁의무)

① 선거에 참여하는 정당·후보자(후보자가 되고자 하는 자를 포함한다. 이하 이 조에서 같다) 및 후보자를 위하여 선거운동을 하는 자는 선거운동을 함에 있어 이 법을 준수하고 공정하게 경쟁하여야 하며, 정당의 정강·정책이나 후보자의 정견을 지지·선전하거나 이를 비판·반대함에 있어 선량한 풍속 기타 사회질서를 해하는 행위를 하여서는 아니된다.

한편, 2008년 중앙선거관리위원회 해석과에서는 예비후보자 현수막 등에 합성사진 게재가 가능한지 여부에 대한 질의에서, "사실과 다른 내용을 게재하는 것은 공직선거법 제250조에 저촉될 것"이라는 해석을 내놓은 바 있다⁸¹⁾. 2006년에는 후보자 본인의 서로 다른 사진 2장을 합성하여 동시에 사용하는 것이 가능한지 여부에 관하여 "후보자 본인의 사진 중 다른 사진 2장을 동시에 사용하는 경우, 후보자만의 사진이라면 무방할 것임"이라 회신한 사례도 있다.

다. 소결

위와 같이 현행 공직선거법에서 딥페이크 기술로 인한 영상에 대해 제250조 허위사실공표죄 또는 제110조 후보자 등의 비방금지 등의 조항이 적용가능하며, 국내에서는 현행 법률 이외에 추가적으로 입법이 진행되고 있는 것은 없다⁸²⁾.

다만 해외에서는 선거 관련하여 딥페이크 영상에 관한 논의가 활발하며 선거일을

81) 2008. 1. 30. 중앙선거관리위원회 위원장 회답

82) 2020. 9. 현재 21대 국회에 계류 중인 공직선거법 일부개정안 42개 가운데 딥페이크 기술을 활용한 허위 영상 등 유포행위를 처벌하는 내용의 개정안은 없는 것으로 파악된다.

기준으로 하여 구체적인 규정을 마련하고 있는바, 현행 공직선거법 상 개선점이 있는지 검토할 필요가 있다.

7. 피해자의 삭제, 처리정지 등 조치요구

가. 서설

위에서 살펴본 바와 같이, 딥페이크 영상의 피해자는 딥페이크 영상의 제작, 유통자 등에 대해 관련 법령에 의한 형사고소, 민사소송 등을 진행할 수 있다. 이러한 소송법적 구제절차는 시일이 오래 소요되며 즉각적인 피해회복이 불가능하다는 단점이 있다.

딥페이크 영상은 피해자의 초상, 음성 등 개인정보를 포함하고 있는바, 피해자는 이러한 개인정보를 근거로 하여 영상의 배포, 유통을 막을 수 있는 법적인 권리가 있다. 개인정보주체는 자신의 얼굴 또는 음성 등이 사용된 딥페이크 영상을 발견한 경우 관련된 개인정보처리자 또는 정보통신서비스 제공자에게 영상의 삭제, 처리정지를 요청할 수 있으며, 요청을 받은 자는 지체없이 삭제, 파기, 접근제한 임시조치 등 필요한 조치를 취해야한다.

이하에서 딥페이크 피해자의 영상 삭제, 처리정지 등 청구권에 대해 살펴보도록 한다.

나. 개인정보보호법

개인정보보호법 상 개인정보란 개인에 관한 정보로서, 성명, 주민등록번호 및 영상 등을 통하여 개인을 알아볼 수 있는 정보를 말한다(동법 제2조 제1호).

개인정보분쟁조정위원회의 조정 사례 가운데 다수의 해석례는 얼굴 사진 등 그 자체만으로(즉, 다른 정보와의 결합 여부에 관계 없이) 개개인을 식별할 수 있는 정보는

개인정보에 해당한다는 입장을 보이고 있다.⁸³⁾

<개인정보분쟁조정위원회 조정 사례 1>

나. 피신청인이 신청인의 개인정보를 침해한 사실이 있는지 여부

신청인은 생존하는 개인으로서 당해 얼굴사진만으로 충분히 신청인 여부를 식별할 수 있는 바, 정보보호법상의 개념을 참고하여 볼 때 신청인의 사진은 개인정보'로 인정될 수 있다.

<개인정보분쟁조정위원회 조정 사례 2>

나. 피신청인이 신청인의 개인정보를 침해한 사실이 있는지 여부

본 사건에서 신청인의 얼굴 전체가 웹사이트에 공개된 것은 아니나 당해 사진만으로도 충분히 신청인 여부를 식별할 수 있으므로, 공개된 신청인의 성형수술 얼굴사진은 정보보호법상 개인정보에 해당된다고 보인다. 특히 공개된 신청인의 얼굴사진은 성형수술 전후의 변화된 모습에 대한 사진인 바, 일종의 의료정보로서 공개될 경우 커다란 수치심을 느낄 수 있는 민감한 개인정보에 해당된다.

법원은 '사람은 누구나 자신의 얼굴 기타 사회통념상 특정인임을 식별할 수 있는 신체적 특징에 관하여 함부로 촬영 또는 그림묘사되는 등으로 공표되지 아니하며 영리적으로 이용당하지 아니할 초상권을 가진다. 이 역시 헌법 제10조 제1문에 의하여 보장되는 권리'(대법원 2013. 6. 27. 선고 2012다31628 판결 참조)라고 본 사례가 있으며, '일반 통행인의 얼굴 등 특정인을 식별할 수 있는 개인에 관한 정보'(대법원 2014. 5. 29. 선고 2012두25729 판결)라 하여, 얼굴 또는 얼굴이 촬영된 영상, 사진 등이 그 자체로 특정인을 식별할 수 있는 정보라는 입장을 보이고 있다.

83) 조정 사례 1은 2003년, 스티커사진 전문점이 고객의 얼굴사진을 무단으로 게재한 건에 대한 조정사례이며, 조정사례 2는 성형외과 병원이 고객의 성형수술 전후사진을 웹사이트에 무단으로 게재한 건에 관한 사례입니다.

위와 같이 딥페이크 영상에는 개인의 초상, 영상, 음성 등이 사용되는데, 딥페이크 영상에서 모방된 초상, 영상, 음성은 개인정보보호법 상 개인정보에 해당한다.

개인정보보호법 제4조에서는 개인정보의 처리 정지, 정정·삭제 및 파기를 요구할 권리가 있다고 규정하고 있다. 이때 개인정보의 처리란 개인정보의 수집, 생성, 연계, 연동, 기록, 저장, 보유, 가공, 편집, 검색, 출력, 정정(訂正), 복구, 이용, 제공, 공개, 파기(破棄), 그 밖에 이와 유사한 행위를 말한다(동법 제2조 제2호).

개인정보보호법

제2조(정의)

이 법에서 사용하는 용어의 뜻은 다음과 같다.

1. "개인정보"란 살아 있는 개인에 관한 정보로서 성명, 주민등록번호 및 영상 등을 통하여 개인을 알아볼 수 있는 정보(해당 정보만으로는 특정 개인을 알아볼 수 없더라도 다른 정보와 쉽게 결합하여 알아볼 수 있는 것을 포함한다)를 말한다.
2. "처리"란 개인정보의 수집, 생성, 연계, 연동, 기록, 저장, 보유, 가공, 편집, 검색, 출력, 정정(訂正), 복구, 이용, 제공, 공개, 파기(破棄), 그 밖에 이와 유사한 행위를 말한다.
5. "개인정보처리자"란 업무를 목적으로 개인정보파일을 운영하기 위하여 스스로 또는 다른 사람을 통하여 개인정보를 처리하는 공공기관, 법인, 단체 및 개인 등을 말한다.

제4조(정보주체의 권리)

정보주체는 자신의 개인정보 처리와 관련하여 다음 각 호의 권리를 가진다.

4. 개인정보의 처리 정지, 정정·삭제 및 파기를 요구할 권리
5. 개인정보의 처리로 인하여 발생한 피해를 신속하고 공정한 절차에 따라 구제받을 권리

개인정보주체는 개인정보처리자가 처리하는 자신의 개인정보에 대한 열람을 요구할 수 있고(개인정보보호법 제35조 제1항), 개인정보를 열람한 정보주체는 개인정보처리자에게 개인정보의 '정정·삭제'를 요구할 수 있다(동법 제36조 제1항). 개인정보처리자는 제36조 제1항에 의한 요구를 받은 경우 지체없이 개인정보를 조사하여 정보주체의 요구에 따라 정정·삭제 등 필요한 조치를 한 후 그 결과를 정보주체에게 알려야 한다(동법 제36조 제2항). 개인정보처리자는 개인정보에 대한 삭제조치를 취할 경우 복구 또는 재생되지 아니하도록 조치하여야 한다(동법 제36조 제3항).

개인정보보호법

제35조(개인정보의 열람)

① 정보주체는 개인정보처리자가 처리하는 자신의 개인정보에 대한 열람을 해당 개인정보처리자에게 요구할 수 있다.

제36조(개인정보의 정정·삭제)

① 제35조에 따라 자신의 개인정보를 열람한 정보주체는 개인정보처리자에게 그 개인정보의 정정 또는 삭제를 요구할 수 있다. 다만, 다른 법령에서 그 개인정보가 수집 대상으로 명시되어 있는 경우에는 그 삭제를 요구할 수 없다.

② 개인정보처리자는 제1항에 따른 정보주체의 요구를 받았을 때에는 개인정보의 정정 또는 삭제에 관하여 다른 법령에 특별한 절차가 규정되어 있는 경우를 제외하고는 지체 없이 그 개인정보를 조사하여 정보주체의 요구에 따라 정정·삭제 등 필요한 조치를 한 후 그 결과를 정보주체에게 알려야 한다.

③ 개인정보처리자가 제2항에 따라 개인정보를 삭제할 때에는 복구 또는 재생되지 아니하도록 조치하여야 한다.

④ 개인정보처리자는 정보주체의 요구가 제1항 단서에 해당될 때에는 지체 없이 그 내용을 정보주체에게 알려야 한다.

⑤ 개인정보처리자는 제2항에 따른 조사를 할 때 필요하면 해당 정보주체에게 정정·삭제 요구사항의 확인에 필요한 증거자료를 제출하게 할 수 있다.

⑥ 제1항·제2항 및 제4항에 따른 정정 또는 삭제 요구, 통지 방법 및 절차 등에 필요한 사항은 대통령령으로 정한다.

개인정보주체는 개인정보처리자에 대하여 자신의 개인정보 처리의 정지를 요구할 수 있다(동법 제37조 제1항). 개인정보처리자는 제37조 제1항에 의한 요구를 받은 경우 지체 없이 정보주체의 요구에 따라 개인정보의 처리의 전부를 정지하거나 일부를 정지하여야 한다(동법 제37조 제2항). 개인정보처리자는 처리가 정지된 개인정보에 대하여 지체 없이 해당 개인정보의 파기 등 필요한 조치를 하여야 한다(동법 제37조 제4항).

개인정보보호법

제37조(개인정보의 처리정지 등)

① 정보주체는 개인정보처리자에 대하여 자신의 개인정보 처리의 정지를 요구할 수

있다. 이 경우 공공기관에 대하여는 제32조에 따라 등록 대상이 되는 개인정보파일 중 자신의 개인정보에 대한 처리의 정지를 요구할 수 있다.

② 개인정보처리자는 제1항에 따른 요구를 받았을 때에는 지체 없이 정보주체의 요구에 따라 개인정보 처리의 전부를 정지하거나 일부를 정지하여야 한다. 다만, 다음 각 호의 어느 하나에 해당하는 경우에는 정보주체의 처리정지 요구를 거절할 수 있다.

1. 법률에 특별한 규정이 있거나 법령상 의무를 준수하기 위하여 불가피한 경우
2. 다른 사람의 생명·신체를 해할 우려가 있거나 다른 사람의 재산과 그 밖의 이익을 부당하게 침해할 우려가 있는 경우
3. 공공기관이 개인정보를 처리하지 아니하면 다른 법률에서 정하는 소관 업무를 수행할 수 없는 경우
4. 개인정보를 처리하지 아니하면 정보주체와 약정한 서비스를 제공하지 못하는 등 계약의 이행이 곤란한 경우로서 정보주체가 그 계약의 해지 의사를 명확하게 밝히지 아니한 경우

③ 개인정보처리자는 제2항 단서에 따라 처리정지 요구를 거절하였을 때에는 정보주체에게 지체 없이 그 사유를 알려야 한다.

④ 개인정보처리자는 정보주체의 요구에 따라 처리가 정지된 개인정보에 대하여 지체 없이 해당 개인정보의 파기 등 필요한 조치를 하여야 한다.

⑤ 제1항부터 제3항까지의 규정에 따른 처리정지의 요구, 처리정지의 거절, 통지 등의 방법 및 절차에 필요한 사항은 대통령령으로 정한다.

위에서 본 바와 같이 딥페이크 영상의 피해자는 개인정보보호법에 근거하여 개인정보처리자인 공공기관, 법인, 단체, 개인 등에 대하여 개인정보가 포함된 딥페이크 영상의 정정·삭제요구, 처리정지요구를 할 수 있다. 개인정보처리자는 위와 같은 정정·삭제요구, 처리정지요구를 받는 즉시 개인정보의 필요한 조치를 취하여야 한다(동법 제35조, 제36조).

참고로, EU에서도 딥페이크 영상의 피해자를 개인정보보호규정(GDPR, General Data Protection Regulation) 제17조 삭제권(잊힐 권리), 제18조 처리제한권에 의하여 보호하고 있다.

다. 정보통신망 이용촉진 및 정보보호 등에 관한 법률

정보통신망법에서는 정보통신망을 통하여 일반에게 공개를 목적으로 제공된 정보로

사생활 침해나 명예훼손 등 타인의 권리가 침해된 경우 그 침해를 받은 자는 해당 정보를 처리한 정보통신서비스 제공자에게 침해사실을 소명하여 그 정보의 삭제 또는 반박내용의 게재(이하 "삭제등"이라 한다)를 요청할 수 있다고 규정하고 있다(제44조의2 제1항).

정보통신서비스 제공자는 제1항에 따른 해당 정보의 삭제 등을 요청받으면 지체 없이 삭제·임시조치 등의 필요한 조치를 하고, 즉시 신청인 및 정보게재자에게 알려야 하며, 필요한 조치를 한 사실을 해당 게시판에 공시하는 등의 방법으로 이용자가 알 수 있도록 하여야 한다(제44조의2 제2항).

정보통신망 이용촉진 및 정보보호 등에 관한 법률

제44조의2(정보의 삭제요청 등)

① 정보통신망을 통하여 일반에게 공개를 목적으로 제공된 정보로 사생활 침해나 명예훼손 등 타인의 권리가 침해된 경우 그 침해를 받은 자는 해당 정보를 처리한 정보통신서비스 제공자에게 침해사실을 소명하여 그 정보의 삭제 또는 반박내용의 게재(이하 "삭제등"이라 한다)를 요청할 수 있다.

② 정보통신서비스 제공자는 제1항에 따른 해당 정보의 삭제등을 요청받으면 지체 없이 삭제·임시조치 등의 필요한 조치를 하고 즉시 신청인 및 정보게재자에게 알려야 한다. 이 경우 정보통신서비스 제공자는 필요한 조치를 한 사실을 해당 게시판에 공시하는 등의 방법으로 이용자가 알 수 있도록 하여야 한다.

제2조(정의)

① 이 법에서 사용하는 용어의 뜻은 다음과 같다.

1. "정보통신망"이란 「전기통신사업법」 제2조제2호에 따른 전기통신설비를 이용하거나 전기통신설비와 컴퓨터 및 컴퓨터의 이용기술을 활용하여 정보를 수집·가공·저장·검색·송신 또는 수신하는 정보통신체제를 말한다.

딥페이크 영상은 주로 인터넷, SNS, 포털사이트, 어플리케이션 등 정보통신망을 통하여 공개되고 있으며, 딥페이크 영상의 내용은 허위로서 사생활침해 또는 명예훼손에 해당할 가능성이 높다. 딥페이크 영상이 정보통신망에 배포됨으로 인해 사생활침해, 명예훼손 등의 피해를 입은 피해자는 해당 인터넷 게시판 운영자, SNS 운영자, 포털사이트 운영자, 어플리케이션 운영자 등 정보통신서비스 제공자에게 침해사실을 소

명하여 해당 영상의 삭제 또는 반박내용의 게재를 요청할 수 있다(제44조의2 제1항). 요청을 받은 정보통신서비스 제공자는 즉시 정보통신망법 상의 필요한 조치를 취하여야 한다(제44조의2 제2항).

라. 성폭력범죄의 처벌 등에 관한 특례법 일부개정법률안

2020. 8. 6. 권인숙의원 등 11인이 성폭력범죄의 처벌 등에 관한 특례법 일부개정법률안(이하 '성폭력처벌법')을 발의하였는데, 위 일부개정법률안은 딥페이크 음란물 피해자의 구제 및 보호 차원에서 피해자와 그 가족이 사생활보호 등의 사유로 불법촬영물과 관련된 증거물의 비공개를 신청할 수 있도록 하는 내용을 담고 있다.

성폭력처벌법위반으로 인한 재판이 진행되는 경우, 피해자의 요청 또는 법원의 직권으로 비공개재판 진행여부를 결정할 수 있으나, 비공개재판으로 진행되더라도 불법촬영물이 증거로 채택되어 비공개재판에 참석한 여러 사람에게 공개되면 피해자가 추가적인 고통을 받을 수 있다. 이에 일부개정법률안은 피해자와 그 가족이 불법촬영물 등 증거물의 비공개를 신청하고, 재판장이 법정 이외의 장소에서 증거물을 열람하도록 하려는 것이다.

성폭력범죄의 처벌 등에 관한 특례법 일부개정법률안 제안이유 및 주요내용

현행법은 성폭력범죄 피해자를 배려하기 위해 조사 및 심리·재판 횟수를 필요한 범위에서 최소한으로 하도록 하고, 피해자의 사생활 보호 등 필요한 경우 법원이 재판 또는 증인신문을 비공개결정을 할 수 있도록 함.

그런데 현행법에 따라 재판이 비공개되더라도 불법촬영물이 증거로 채택되어 가족 등 여러 사람에게 공개되면 피해자에게 추가적인 고통을 줄 수 있음. 증인신문과 같이 증거물 또한 피해자와 그 가족이 비공개를 신청할 필요가 있으나, 이에 대한 규정이 미비한 상황임.

이에 피해자와 그 가족이 증거물의 비공개를 신청하고, 재판장은 법정 외의 장소에서 증거물을 열람하도록 하려는 것임(안 제31조).

구체적으로 성폭력처벌법 일부개정법률안은 제31조 제3항을 신설할 것을 제안하고

있다. 제31조 제3항은 성폭력범죄의 피해자와 그 가족은 사생활보호 등의 사유로 증거물의 비공개를 신청할 수 있다고 규정하고 있다.

<표 3-2> 성폭력처벌법 일부개정법률안 신구조문 대비표

현행	개정안
제31조(심리의 비공개) ①·② (생략)	제31조(심리 등의 비공개) ①·② (현행과 같음)
<신설>	③ 성폭력범죄의 피해자와 그 가족은 사생활보호 등의 사유로 증거물의 비공개를 신청할 수 있다.
③ 재판장은 제2항에 따른 신청을 받으면 그 허가 및 공개 여부, 법정 외의 장소에서의 신문 등 증인의 신문 방식 및 장소에 관하여 결정할 수 있다.	④ -----제2항 및 제3항에 -----신문 또는 증거물 열람 등 증인신문 과 증거물 열람 방식 -----.
④ 제1항 및 제3항의 경우에는 「법원조직법」 제57조(재판의 공개)제2항·제3항 및 「군사법원법」 제67조제2항·제3항을 준용한다.	⑤ -----제4항의 -----.

성폭력처벌법 제14조의2에서는 딥페이크 기술로 생성한 허위 음란영상물을 규제하고 있는바, 위 일부개정법률안 제31조 제3항 상 성폭력범죄의 피해자에는 딥페이크 영상의 피해자가 포함된다. 위 일부개정법률안이 시행되는 경우 딥페이크 영상의 피해자는 딥페이크 영상이 재판의 증거로 사용되는 경우 영상의 비공개를 신청할 수 있게 된다.

마. 소결

위에서 본 바와 같이 딥페이크 영상의 개인의 초상, 영상, 음성은 개인정보보호법상 개인정보에 해당하는바, 개인정보주체는 개인정보처리자에 대하여 개인정보가 포함된 딥페이크 영상의 정정·삭제요구, 처리정지요구를 할 수 있다(개인정보보호법 제35조, 제36조).

또한 딥페이크 영상이 정보통신망에 배포됨으로 인해 사생활침해, 명예훼손 등의 피해를 입은 피해자는 정보통신서비스 제공자에게 침해사실을 소명하여 해당 영상의 삭제 또는 반박내용의 게재를 요청할 수 있다(정보통신망법 제44조의2).

한편, 2020. 8. 6. 권인숙의원 등 11인에 의해 성폭력처벌법 일부개정법률안이 발의되었는바, 위 일부개정법률안에 따라 제31조 제3항이 신설되는 경우 딥페이크 영상의 피해자는 딥페이크 영상이 재판의 증거로 사용되는 경우 영상의 비공개를 신청할 수 있게 된다.

이처럼 딥페이크 영상의 피해자는 개인정보보호법, 정보통신망법 등에 의하여 딥페이크 영상에 대한 정정·삭제요구, 처리정지요구, 반박내용 게재요구 등이 가능하다.

현재 국내 법령 상 피해자가 정보의 정정·삭제·처리정지 등을 요구할 수 있는 절차가 마련되어 있어 입법 공백이 없는 것으로 보인다.

8. 플랫폼 운영자의 책임과 의무

가. 서설

딥페이크 영상은 개인 간 통신행위 뿐만 아니라 인터넷, SNS, 포털사이트, 어플리케이션 등 정보통신망을 통하여 유통될 수 있는바, 이때 인터넷 게시판 운영자, SNS 운영자, 포털사이트 운영자, 어플리케이션 운영자 등(이하 '플랫폼 운영자'라 한다)의 의

무와 책임이 문제된다.

나. 정보통신망 이용촉진 및 정보보호 등에 관한 법률

1) 플랫폼 운영자의 불법정보 유통금지 의무

정보통신망법에서는 제44조 제1항에서는 이용자가 사생활 침해 또는 명예훼손 등 타인의 권리를 침해하는 정보를 유통시켜서는 안 된다고 규정하면서, 제44조 제2항에서 정보통신서비스 제공하는 자신이 운영·관리하는 정보통신망에 제1항에 따른 정보가 유통되지 아니하도록 노력하여야 한다고 규정하고 있다. 다만 노력하여야 한다면 고 하여 권고적인 수준에 그치고 있을 뿐 이를 법적으로 강제하고 있지는 아니하다.

정보통신망 이용촉진 및 정보보호 등에 관한 법률

제44조(정보통신망에서의 권리보호)

- ① 이용자는 사생활 침해 또는 명예훼손 등 타인의 권리를 침해하는 정보를 정보통신망에 유통시켜서는 아니 된다.
- ② 정보통신서비스 제공자는 자신이 운영·관리하는 정보통신망에 제1항에 따른 정보가 유통되지 아니하도록 노력하여야 한다.

정보통신망법에서는 제44조의7 제1항에서는 누구든지 정보통신망을 통하여, 음란한 부호·문언·음향·화상 또는 영상을 배포·판매·임대하거나 공공연하게 전시하는 내용의 정보(제1호), 사람을 비방할 목적으로 공공연하게 사실이나 거짓의 사실을 드러내어 타인의 명예를 훼손하는 내용의 정보(제2호), 공포심이나 불안감을 유발하는 부호·문언·음향·화상 또는 영상을 반복적으로 상대방에게 도달하도록 하는 내용의 정보(제4호), 그 밖에 범죄를 목적으로 하거나 교사(敎唆) 또는 방조하는 내용의 정보(제5호)를 유통하여서는 안 된다고 규정하고 있다.

딥페이크 영상은 음란한 음향 또는 영상, 타인의 명예를 훼손하는 정보, 공포심이나 불안감을 유발하는 음향 또는 영상, 그 밖에 범죄를 목적으로 하거나 교사 또는 방조하는 내용의 정보에 해당할 가능성이 있다.

정보통신망법 제44조의7 제2항은 음란한 음향 또는 영상(제44조의7 제1항 제1호), 명예훼손 정보(제44조의7 제1항 제1호), 공포심이나 불안감을 유발하는 음향 또는 영상(제44조의7 제1항 제1호)의 정보의 경우, 방송통신위원회가 심의위원회의 심의를 거쳐 정보통신서비스 제공자 또는 게시관 관리·운영자로 하여금 그 처리를 거부·정지 또는 제한하도록 명할 수 있다고 규정하고 있다.

정보통신망법 제44조의7 제3항은 그 밖에 범죄를 목적으로 하거나 교사 또는 방조하는 내용의 정보(제44조의7 제9호)의 경우, 제44조의7 제3항 각 호의 요건을 충족하는 경우 정보통신서비스 제공자 또는 게시관 관리·운영자에게 해당 정보의 처리를 거부·정지 또는 제한하도록 명하여야 한다고 규정하고 있다. 제44조의7 제3항 제1호는 관계 중앙행정기관의 장의 요청[제1항제9호의 정보 중 성폭력범죄의 처벌 등에 관한 특례법 제14조에 따른 촬영물 또는 복제물(복제물의 복제물을 포함한다)에 대하여는 수사기관의 장의 요청을 포함한다]이 있었을 것을 요건하고 하고 있는바, 제9호의 영상에는 성폭력처벌법 제14조의 음란영상물이 포함될 것이 예정되어 있다고 하겠다. 성폭력처벌법 제14조의2가 최근 신설 되었음에도 제44조의7 제3항에는 반영되어 있지 않은바 이는 입법공백일 가능성이 높다.

정보통신망 이용촉진 및 정보보호 등에 관한 법률

제44조의7(불법정보의 유통금지 등)

① 누구든지 정보통신망을 통하여 다음 각 호의 어느 하나에 해당하는 정보를 유통하여서는 아니 된다.

1. 음란한 부호·문언·음향·화상 또는 영상을 배포·판매·임대하거나 공공연하게 전시하는 내용의 정보
2. 사람을 비방할 목적으로 공공연하게 사실이나 거짓의 사실을 드러내어 타인의 명예를 훼손하는 내용의 정보
3. 공포심이나 불안감을 유발하는 부호·문언·음향·화상 또는 영상을 반복적으로 상대방에게 도달하도록 하는 내용의 정보
7. 법령에 따라 분류된 비밀 등 국가기밀을 누설하는 내용의 정보
8. 「국가보안법」에서 금지하는 행위를 수행하는 내용의 정보
9. 그 밖에 범죄를 목적으로 하거나 교사(敎唆) 또는 방조하는 내용의 정보

② 방송통신위원회는 제1항제1호부터 제6호까지, 제6호의2 및 제6호의3의 정보에 대

하여는 심의위원회의 심의를 거쳐 정보통신서비스 제공자 또는 게시판 관리·운영자로 하여금 그 처리를 거부·정지 또는 제한하도록 명할 수 있다. 다만, 제1항제2호 및 제3호에 따른 정보의 경우에는 해당 정보로 인하여 피해를 받은 자가 구체적으로 밝힌 의사에 반하여 그 처리의 거부·정지 또는 제한을 명할 수 없다.

③ 방송통신위원회는 제1항제7호부터 제9호까지의 정보가 다음 각 호의 모두에 해당하는 경우에는 정보통신서비스 제공자 또는 게시판 관리·운영자에게 해당 정보의 처리를 거부·정지 또는 제한하도록 명하여야 한다.

1. 관계 중앙행정기관의 장의 요청[제1항제9호의 정보 중 「성폭력범죄의 처벌 등에 관한 특례법」 제14조에 따른 촬영물 또는 복제물(복제물의 복제물을 포함한다)에 대하여는 수사기관의 장의 요청을 포함한다]이 있었을 것

2. 제1호의 요청을 받은 날부터 7일 이내에 심의위원회의 심의를 거친 후 「방송통신위원회의 설치 및 운영에 관한 법률」 제21조제4호에 따른 시정 요구를 하였을 것

3. 정보통신서비스 제공자나 게시판 관리·운영자가 시정 요구에 따르지 아니하였을 것

④ 방송통신위원회는 제2항 및 제3항에 따른 명령의 대상이 되는 정보통신서비스 제공자, 게시판 관리·운영자 또는 해당 이용자에게 미리 의견제출의 기회를 주어야 한다. 다만, 다음 각 호의 어느 하나에 해당하는 경우에는 의견제출의 기회를 주지 아니할 수 있다.

1. 공공의 안전 또는 복리를 위하여 긴급히 처분을 할 필요가 있는 경우

2. 의견청취가 뚜렷이 곤란하거나 명백히 불필요한 경우로서 대통령령으로 정하는 경우

3. 의견제출의 기회를 포기한다는 뜻을 명백히 표시한 경우

2) 불법정보 삭제·임시조치 등

정보통신망법에서는 정보통신망을 통하여 일반에게 공개를 목적으로 제공된 정보로 사생활 침해나 명예훼손 등 타인의 권리가 침해된 경우 그 침해를 받은 자는 해당 정보를 처리한 정보통신서비스 제공자에게 침해사실을 소명하여 그 정보의 삭제 또는 반박내용의 게재(이하 "삭제등"이라 한다)를 요청할 수 있다고 규정하고 있다(제44조의2 제1항).

정보통신서비스 제공자가 제1항에 따른 해당 정보의 삭제 등을 요청받은 경우 지체 없이 삭제·임시조치 등의 필요한 조치를 하고, 즉시 신청인 및 정보게재자에게 알려야 하며, 필요한 조치를 한 사실을 해당 게시판에 공시하는 등의 방법으로 이용자가

알 수 있도록 하여야 한다(제44조의2 제2항).

정보통신서비스 제공자는 제44조의2 제1항에 따른 정보의 삭제요청에도 불구하고 권리의 침해 여부를 판단하기 어렵거나 이해당사자 간에 다툼이 예상되는 경우에는 해당 정보에 대한 접근을 임시적으로 차단하는 조치(이하 "임시조치"라 한다)를 할 수 있다. 이 경우 임시조치의 기간은 30일 이내로 한다(제44조의2 제4항). 정보통신서비스 제공자는 필요한 조치에 관한 내용·절차 등을 미리 약관에 구체적으로 밝혀야 한다(제44조의2 제5항).

정보통신서비스 제공자는 자신이 운영·관리하는 정보통신망에 유통되는 정보에 대하여 제44조의2 제2항에 따른 필요한 조치를 하면 이로 인한 배상책임을 줄이거나 면제받을 수 있다(제44조의2 제6항).

정보통신망 이용촉진 및 정보보호 등에 관한 법률

제44조의2(정보의 삭제요청 등)

- ① 정보통신망을 통하여 일반에게 공개를 목적으로 제공된 정보로 사생활 침해나 명예훼손 등 타인의 권리가 침해된 경우 그 침해를 받은 자는 해당 정보를 처리한 정보통신서비스 제공자에게 침해사실을 소명하여 그 정보의 삭제 또는 반박내용의 게재(이하 "삭제등"이라 한다)를 요청할 수 있다.
- ② 정보통신서비스 제공자는 제1항에 따른 해당 정보의 삭제등을 요청받으면 지체 없이 삭제·임시조치 등의 필요한 조치를 하고 즉시 신청인 및 정보게재자에게 알려야 한다. 이 경우 정보통신서비스 제공자는 필요한 조치를 한 사실을 해당 게시판에 공시하는 등의 방법으로 이용자가 알 수 있도록 하여야 한다.
- ④ 정보통신서비스 제공자는 제1항에 따른 정보의 삭제요청에도 불구하고 권리의 침해 여부를 판단하기 어렵거나 이해당사자 간에 다툼이 예상되는 경우에는 해당 정보에 대한 접근을 임시적으로 차단하는 조치(이하 "임시조치"라 한다)를 할 수 있다. 이 경우 임시조치의 기간은 30일 이내로 한다.
- ⑤ 정보통신서비스 제공자는 필요한 조치에 관한 내용·절차 등을 미리 약관에 구체적으로 밝혀야 한다.
- ⑥ 정보통신서비스 제공자는 자신이 운영·관리하는 정보통신망에 유통되는 정보에 대하여 제2항에 따른 필요한 조치를 하면 이로 인한 배상책임을 줄이거나 면제받을 수 있다.

정보통신서비스 제공자는 제44조의2 제1항과 같이 권리침해자의 요청을 받지 아니한 경우에도, 자신이 운영·관리하는 정보통신망에 유통되는 정보가 사생활 침해 또는 명예훼손 등 타인의 권리를 침해한다고 인정되면 임의로 임시조치를 할 수 있다(제44조의3 제1항).

정보통신서비스 제공자가 임의로 임시조치를 한 경우 필요한 조치를 취한 사실을 해당 게시판에 게시하는 등의 방법으로 이용자가 알도록 해야 하며, 임시조치의 기간은 30일 이내로 하여야 하고, 필요한 조치에 관한 내용·절차 등을 미리 약관에 구체적으로 밝혀야 한다(제44조의3 제2항, 제44조의2 제2항 후단, 제4항 후단 및 제5항).

정보통신망 이용촉진 및 정보보호 등에 관한 법률

제44조의3(임의의 임시조치)

- ① 정보통신서비스 제공자는 자신이 운영·관리하는 정보통신망에 유통되는 정보가 사생활 침해 또는 명예훼손 등 타인의 권리를 침해한다고 인정되면 임의로 임시조치를 할 수 있다.
- ② 제1항에 따른 임시조치에 관하여는 제44조의2제2항 후단, 제4항 후단 및 제5항을 준용한다.

참고로, 독일은 소셜네트워크상의 법집행 개선에 관한 법률(Gesetz zur Verbesserung der Rechtsdurchsetzung in sozialen Netzwerken, 네트워크 법집행법)에서 회원수가 2백만 명 이상인 소셜네트워크 운영자에게 위법한 콘텐츠에 대한 삭제 조치 등의 의무를 지우고 있으나(§ 1), 정보통신망법에서는 정보통신서비스 제공자의 규모를 제한하지 아니하고 모든 정보통신서비스 제공자를 대상으로 하고 있다. 중국의 네트워크 오디오 및 비디오 정보 서비스 관리규정(网络音视频信息服务管理规定, Regulations on the Administration of Network Audio and Video Information Services) 또한 온라인 오디오·영상정보서비스 제공자의 규모를 특별히 제한하지 않고 있다.

3) 불법촬영물등 유통방지 책임자 지정

한편, 정보통신망법 일부개정법률안은 2020. 6. 29. 공포되어 2020. 12. 10.부터 시행 예정인데, 위 개정법률안이 딥페이크 관련 쟁점을 담고 있다.

개정된 정보통신망법 제44조의9 제1항은 정보통신서비스 제공자 중 일일 평균 이용자의 수, 매출액, 사업의 종류 등이 대통령령으로 정하는 기준에 해당하는 자는 자신이 운영·관리하는 정보통신망을 통하여 일반에게 공개되어 유통되는 정보 각 호의 정보의 유통을 방지하기 위한 책임자(이하 "불법촬영물등 유통방지 책임자"라 한다)를 지정하여야 한다고 규정하면서, 제2호에서 성폭력처벌법 제14조의2의 편집물·합성물·가공물 또는 복제물을 규정하고 있다.

성폭력처벌법 제14조의2는 허위 음란영상물의 제작에 관한 규정으로 딥페이크 기술로 제작한 허위 음란영상물이 포함된다. 따라서 대통령령으로 정하는 일정규모 이상의 정보통신서비스 이용자는 딥페이크 기술로 제작한 허위 음란영상물의 유통을 방지하기 위한 책임자를 지정하여야 한다⁸⁴⁾.

불법촬영물등 유통방지 책임자는 전기통신사업법 제22조의5 제1항에 따른 불법촬영물등의 삭제·접속차단 등 유통방지에 필요한 조치 업무를 수행하여야 하는데(동법 제44조의9 제2항), 전기통신사업법 제22조의5 제1항에서는 성폭력처벌법 제14조의2에 따른 편집물·합성물·가공물 또는 복제물을 불법촬영물등으로 정의하고 있다. 따라서 불법촬영물등 유통방지 책임자의 업무범위에 딥페이크 기술로 제작한 허위 음란영상물도 포함된다.

정보통신망법 제44조의9 제1항을 위반하는 경우 2천만원 이하의 과태료에 처해진다(동법 제 76조 제2항 제4의4호).

불법촬영물등 유통방지 책임자의 수 및 자격요건, 불법촬영물등 유통방지 책임자에 대한 교육 등에 관하여 필요한 사항은 대통령령으로 정하도록 되어 있으나(동법 제44

84) 참고로 중국 네트워크 오디오 및 비디오 정보 서비스 관리규정(网络音视频信息服务管理规定, Regulations on the Administration of Network Audio and Video Information Services)은 온라인 오디오·영상정보서비스 제공자에게 정보보안관리에 대한 일반적인 감독 의무와 전문가를 임명하여 보안사고 및 불법, 범죄 행위를 방지할 의무를 부과하고 있다(제7조).

조의9 제3항), 아직 대통령령이 제정되지 아니한 상태이다.

참고로, 독일은 소셜네트워크상의 법집행 개선에 관한 법률(Gesetz zur Verbesserung der Rechtsdurchsetzung in sozialen Netzwerken, 네트워크 법집행법)에서 회원수가 2백만 명 이상인 소셜네트워크 운영자에게 각종 의무를 지우고 있다(§ 1).

정보통신망 이용촉진 및 정보보호 등에 관한 법률

제44조의9(불법촬영물등 유통방지 책임자)

① 정보통신서비스 제공자 중 일일 평균 이용자의 수, 매출액, 사업의 종류 등이 대통령령으로 정하는 기준에 해당하는 자는 자신이 운영·관리하는 정보통신망을 통하여 일반에게 공개되어 유통되는 정보 중 다음 각 호의 정보(이하 “불법촬영물등”이라 한다)의 유통을 방지하기 위한 책임자(이하 “불법촬영물등 유통방지 책임자”라 한다)를 지정하여야 한다.

2. 「성폭력범죄의 처벌 등에 관한 특례법」 제14조의2에 따른 편집물·합성물·가공물 또는 복제물(복제물의 복제물을 포함한다)

3. 「아동·청소년의 성보호에 관한 법률」 제2조제5호에 따른 아동·청소년성착취물

② 불법촬영물등 유통방지 책임자는 「전기통신사업법」 제22조의5제1항에 따른 불법촬영물등의 삭제·접속차단 등 유통방지에 필요한 조치 업무를 수행한다.

③ 불법촬영물등 유통방지 책임자의 수 및 자격요건, 불법촬영물등 유통방지 책임자에 대한 교육 등에 관하여 필요한 사항은 대통령령으로 정한다.

제76조(과태료)

② 다음 각 호의 어느 하나에 해당하는 자에게는 2천만원 이하의 과태료를 부과한다.

4의4. 제44조의9제1항을 위반하여 불법촬영물등 유통방지 책임자를 지정하지 아니한 자

전기통신사업법

제22조의5(부가통신사업자의 불법촬영물 등 유통방지)

① 제22조제1항에 따라 부가통신사업을 신고한 자(제22조제4항 각 호의 어느 하나에 해당하는 자를 포함한다) 및 특수유형부가통신사업자 중 제22조제14호가목에 해당하는 자(이하 “조치의무사업자”라 한다)는 자신이 운영·관리하는 정보통신망을 통하여 일반에게 공개되어 유통되는 정보 중 다음 각 호의 정보(이하 “불법촬영물등”이라 한다)가 유통되는 사정을 신고, 삭제요청 또는 대통령령으로 정하는 기관·단체의 요청 등

을 통하여 인식한 경우에는 지체 없이 해당 정보의 삭제·접속차단 등 유통방지에 필요한 조치를 취하여야 한다.

2. 「성폭력범죄의 처벌 등에 관한 특례법」 제14조의2에 따른 편집물·합성물·가공물 또는 복제물(복제물의 복제물을 포함한다)

4) 투명성 보고서 작성 및 제출

개정된 정보통신망법 제64조의5 제1항은 정보통신서비스 제공자 중 일일 평균 이용자의 수, 매출액, 사업의 종류 등이 대통령령으로 정하는 기준에 해당하는 자⁸⁵⁾는 매년 자신이 제공하는 정보통신서비스를 통하여 유통되는 불법촬영물등의 처리에 관하여 각 호의 사항을 포함한 보고서(이하 "투명성 보고서"라 한다)를 작성하여 다음해 1월 31일까지 방송통신위원회에 제출하여야 한다고 규정하고 있다.

제64조의5 제1항 제1호는 정보통신서비스 제공자가 불법촬영물등의 유통 방지를 위하여 기울인 일반적인 노력에 관한 사항, 제2호는 전기통신사업법 제22조의5 제1항에 따른 불법촬영물등의 신고, 삭제요청 등의 횟수, 내용, 처리기준, 검토결과 및 처리결과에 관한 사항, 제3호는 전기통신사업법 제22조의5 제1항에 따른 불법촬영물등의 삭제·접속차단 등 유통방지에 필요한 절차의 마련 및 운영에 관한 사항, 제4호는 불법촬영물등 유통방지 책임자의 배치에 관한 사항, 제5호는 불법촬영물등 유통방지를 위한 내부 교육의 실시와 지원에 관한 사항이다.

위 불법촬영물등에는 딥페이크 기술로 제작한 허위 음란영상물이 포함되므로, 일정 규모이상의 정보통신서비스 제공자는 딥페이크 기술로 제작한 허위 음란영상물의 처리에 관하여 투명성보고서를 작성한 후 방송통신위원회에 제출하여야 한다.

정보통신망법 제64조의5 제1항을 위반하는 경우 1천만원 이하의 과태료에 처해진다(동법 제 76조 제3항 제25호).

한편, 방송통신위원회는 위와 같이 제출된 투명성 보고서를 자신이 운영·관리하는

85) 아직 대통령령이 제정되지 아니한 상태이다.

정보통신망을 통하여 공개하여야 하며(제64조의5 제2항), 투명성 보고서의 사실을 확인하거나 제출된 자료의 진위를 확인하기 위하여 정보통신서비스제공자에게 자료의 제출을 요구할 수 있다(제64조의5 제3항).

정보통신망 이용촉진 및 정보보호 등에 관한 법률

제64조의5(투명성 보고서 제출의무 등)

① 정보통신서비스 제공자 중 일일 평균 이용자의 수, 매출액, 사업의 종류 등이 대통령령으로 정하는 기준에 해당하는 자는 매년 자신이 제공하는 정보통신서비스를 통하여 유통되는 불법촬영물등의 처리에 관하여 다음 각 호의 사항을 포함한 보고서(이하 “투명성 보고서”라 한다)를 작성하여 다음해 1월 31일까지 방송통신위원회에 제출하여야 한다.

1. 정보통신서비스 제공자가 불법촬영물등의 유통 방지를 위하여 기울인 일반적인 노력에 관한 사항
2. 「전기통신사업법」 제22조의5제1항에 따른 불법촬영물등의 신고, 삭제요청 등의 횟수, 내용, 처리기준, 검토결과 및 처리결과에 관한 사항
3. 「전기통신사업법」 제22조의5제1항에 따른 불법촬영물등의 삭제·접속차단 등 유통방지에 필요한 절차의 마련 및 운영에 관한 사항
4. 불법촬영물등 유통방지 책임자의 배치에 관한 사항
5. 불법촬영물등 유통방지를 위한 내부 교육의 실시와 지원에 관한 사항

② 방송통신위원회는 투명성 보고서를 자신이 운영·관리하는 정보통신망을 통하여 공개하여야 한다.

③ 방송통신위원회는 투명성 보고서의 사실을 확인하거나 제출된 자료의 진위를 확인하기 위하여 정보통신서비스제공자에게 자료의 제출을 요구할 수 있다.

제76조(과태료)

③ 다음 각 호의 어느 하나에 해당하는 자에게는 1천만원 이하의 과태료를 부과한다.

25. 제64조의5제1항을 위반하여 투명성 보고서를 제출하지 아니한 자

다. 전기통신사업법

최근 인터넷 사업자의 디지털 성범죄물 유통방지 의무 강화를 골자로 하는 2020. 6. 9. 자 전기통신사업법 일부개정안이 통과되어, 2020. 12. 10. 시행을 앞두고 있다. 전기통신사업법 개정안은 디지털 성범죄물에 딥페이크 기술을 활용한 편집물, 합성물,

가공물 등을 추가하였다.

전기통신사업법 제22조의5 제1항은 동법 제22조제1항에 따라 부가통신사업을 신고한 자(제22조제4항 각 호의 어느 하나에 해당하는 자를 포함한다) 및 특수유형부가통신사업자 중 제2조 제14호가목에 해당하는 자(이하 "조치의무사업자"라 한다)는 자신이 운영·관리하는 정보통신망을 통하여 일반에게 공개되어 유통되는 정보 중 각 호의 정보(이하 "불법촬영물등"이라 한다)가 유통되는 사정을 신고, 삭제요청 또는 대통령령으로 정하는 기관·단체의 요청 등을 통하여 인식한 경우에는 지체 없이 해당 정보의 삭제·접속차단 등 유통방지에 필요한 조치를 취하여야 한다고 규정하고 있다.

기존 전기통신사업법 제22조의5 제 1항은 제1호에서 성폭력처벌법 제14조만을 규정하고 있었으나, 최근 허위영상물에 관한 제14조의2가 신설되면서, 전기통신사업법 제22조의5 제1항 제2호에 성폭력처벌법 제14조의2가 추가되었다.

전기통신사업법

제22조의5(부가통신사업자의 불법촬영물 등 유통방지)

① 제22조제1항에 따라 부가통신사업을 신고한 자(제22조제4항 각 호의 어느 하나에 해당하는 자를 포함한다) 및 특수유형부가통신사업자 중 제2조제14호가목에 해당하는 자(이하 "조치의무사업자"라 한다)는 자신이 운영·관리하는 정보통신망을 통하여 일반에게 공개되어 유통되는 정보 중 다음 각 호의 정보(이하 "불법촬영물등"이라 한다)가 유통되는 사정을 신고, 삭제요청 또는 대통령령으로 정하는 기관·단체의 요청 등을 통하여 인식한 경우에는 지체 없이 해당 정보의 삭제·접속차단 등 유통방지에 필요한 조치를 취하여야 한다.

1. 「성폭력범죄의 처벌 등에 관한 특례법」 제14조에 따른 촬영물 또는 복제물(복제물의 복제물을 포함한다)
2. 「성폭력범죄의 처벌 등에 관한 특례법」 제14조의2에 따른 편집물·합성물·가공물 또는 복제물(복제물의 복제물을 포함한다)

이로써 딥페이크 기술을 활용한 음란영상물의 편집, 합성, 가공 행위 처벌 수위를 강화하는 내용의 2020. 5. 19.자 성폭력범죄의 처벌 등에 관한 특례법 개정에 발맞추어, 전기통신사업자는 딥페이크 기술을 활용한 합성 영상 등에 대해서도 삭제, 접속차단 등 유통방지 조치의무와 기술적, 관리적 조치의무를 부담하게 되었다.

전기통신사업법 제22조의5 제1항을 위반한 자에게는 대통령령으로 정하는 매출액의 100분의 3 이하에 해당하는 금액을 과징금으로 부과할 수 있다(전기통신사업법 제22조의6 제1항).

전기통신사업법

제22조의6(유통방지 조치 등 미이행에 대한 과징금의 부과)

- ① 방송통신위원회는 제22조의5제1항에 따른 불법촬영물등의 삭제·접속차단 등 유통방지에 필요한 조치를 의도적으로 취하지 아니한 자에게 대통령령으로 정하는 매출액의 100분의 3 이하에 해당하는 금액을 과징금으로 부과할 수 있다.
- ② 방송통신위원회는 조치의무사업자가 매출액 산정 자료의 제출을 거부하거나 거짓 자료를 제출하면 해당 조치의무사업자 및 동종 유사 역무제공사업자의 재무제표 등 회계 자료와 가입자 수 및 이용요금 등 영업 현황 자료에 근거하여 매출액을 추정할 수 있다. 다만, 매출액이 없거나 매출액을 산정하기 곤란한 경우로서 대통령령으로 정하는 경우에는 10억원 이하의 과징금을 부과할 수 있다.
- ③ 제1항 및 제2항에 따른 과징금의 구체적인 부과기준은 대통령령으로 정한다.
- ④ 제1항 및 제2항에 따른 과징금의 가산금, 독촉·징수 및 환급가산금에 관하여는 제53조제5항부터 제9항까지의 규정을 준용한다.
- ⑤ 방송통신위원회가 제1항 및 제2항에 따라 과징금을 부과한 경우에는 「방송통신위원회의 설치 및 운영에 관한 법률」 제18조에 따른 방송통신심의위원회에 그 사실을 통보한다.

이와 같이 전기통신사업법 제22조의5 제1항에 따라 부가통신사업을 신고한 자 및 특수유형부가통신사업자는 자신이 운영·관리하는 정보통신망을 통하여 일반에게 공개되어 유통되는 딥페이크 기술로 만든 음란영상물이 유통되는 사정을 신고, 삭제요청 또는 대통령령으로 정하는 기관·단체의 요청 등을 통하여 인식한 경우에는 지체 없이 해당 정보의 삭제·접속차단 등 유통방지에 필요한 조치를 취하여야 하며, 조치를 취하지 않은 경우 과징금에 처해진다.

라. 소결

인터넷 게시판 운영자, SNS 운영자, 포털사이트 운영자, 어플리케이션 운영자 등의

플랫폼 운영자는 정보통신망법 상 정보통신서비스 제공자, 전기통신사업법 제22조의5 제1항의 적용을 받는 사업자에 해당할 수 있다.

정보통신망법은 플랫폼 운영자로 하여금 자신이 운영하는 정보통신망에 사생활 침해 또는 명예훼손 등 타인의 권리를 침해하는 정보가 유통되지 않도록 노력할 것을 규정하고 있으며(동법 제44조 제1항), 음란한 음향 또는 영상(제44조의7 제1항 제1호), 명예훼손 정보(제44조의7 제1항 제1호), 공포심이나 불안감을 유발하는 음향 또는 영상(제44조의7 제1항 제1호)의 정보의 경우, 방송통신위원회가 심의위원회의 심의를 거쳐 정보통신서비스 제공자 또는 게시판 관리·운영자로 하여금 그 처리를 거부·정지 또는 제한하도록 명할 수 있다고 규정하고 있다(제44조의7 제2항). 또한 성폭력처벌법 제14조 상의 음란물 등의 경우 일정요건을 갖추면, 방송통신위원회가 정보통신서비스 제공자 또는 게시판 관리·운영자에게 해당 정보의 처리를 거부·정지 또는 제한하도록 명할 수 있도록 규정하고 있다(제44조의7 제3항).

한편, 정보통신망법은 사생활 침해 또는 명예훼손 등으로 권리가 침해된 자가 정보의 삭제 또는 반박내용의 게재를 요청한 경우, 지체 없이 삭제·임시조치 등의 필요한 조치를 취하고, 조치내용을 신청인 또는 정보게재자에게 알리며, 조치사실을 해당 게시판에 공시하는 등의 방법으로 이용자가 알 수 있도록 하여야 한다고 규정하고 있다(동법 제44조의2 제2항). 플랫폼 사업자가 제44조의2 제2항에 따른 필요한 조치를 취하면 이로 인한 배상책임을 줄이거나 면제받을 수 있다(제44조의2 제6항).

플랫폼 운영자는 권리 침해여부를 판단하기 어려운 등의 경우에는 해당 정보에 대한 접근을 임시적으로 차단하는 임시조치를 취할 수 있으며(제44조의2 제4항), 권리자의 요청을 받지 아니한 경우에도 해당 정보가 사생활 침해 또는 명예훼손 등 타인의 권리를 침해한다고 판단되면 임시조치를 취할 수 있다(제44조의3 제1항).

나아가 정보통신망법은 최근 법률개정을 통하여, 일정규모 이상의 정보통신서비스 제공자로 하여금 딥페이크 기술로 생성된 음란물의 유통을 방지하기 위한 책임자를 지정하고(동법 제44조의 9), 불법촬영물 등의 유통방지와 관련된 각종 사항에 대한 보고서 작성 및 제출 의무를 부여하였다(동법 제64조의5).

전기통신사업법에서는 플랫폼 운영자로 하여금 딥페이크 기술로 제작된 허위 음란 영상물에 대한 삭제·접속차단 등 유통방지에 필요한 조치를 취하도록 규정하고 있다(전기통신사업법 제22조의5 제1항).

위와 같이 현행 국내 법령은 플랫폼 사업자의 조치의무, 조치의 구체적인 내용, 플랫폼 사업자의 면책범위 등에 관하여 입법 공백이 없는 상황이며, 최근 플랫폼 운영자의 불법촬영물등 유통방지 책임자 지정, 투명성 보고서 작성 의무 등이 추가되어 더욱 충실한 입법이 된 상황이다.

다만 플랫폼 운영자가 딥페이크 기술로 제작한 음란영상물 유통이 될 것임을 알고 고의적으로 플랫폼을 제공한 경우에 대한 형사처벌이 없는 것이 문제될 수 있으나⁸⁶⁾, 이는 성폭력처벌법 제14조의2의 공범 또는 방조범으로 해결이 가능할 것으로 보이며, 그 외 명예훼손 정보를 담은 딥페이크 영상 등에도 기존 형사처벌규정에 대한 공범 또는 방조범 처벌규정으로 해결이 가능할 것으로 보인다.

한편, 정보통신망법 제44조의7 제3항 제1호에서 성폭력처벌법 제14조만을 규정하고 있을 뿐, 최근 신설된 제14조의2는 포함하지 않고 있어 이를 입법공백으로 볼 여지가 있다.

9. 정부의 시책마련

86) 참고로, 미국의 온라인 성매매 퇴치법(Allow States and Victims to Fight Online Sex Trafficking Act)은 온라인 성매매 알선이 이뤄지는 '상호 컴퓨터 서비스(interactive computer service)'의 소유·관리·운영자에 대하여 형사처벌하고 있으며, 플랫폼 사업자가 온라인 성매매 알선이 이루어지는 플랫폼을 제공한 경우 형사처벌의 대상이 된다(SEC. 3. (a),(b)). 피해자는 플랫폼 사업자에게 민사상 손해배상을 청구할 수 있고(온라인 성매매 퇴치법 SEC. 3. (c)), 법원은 배상명령을 할 의무가 있다(온라인 성매매 퇴치법 SEC. 3. (d)).

가. 서설

지금까지 음란물, 명예훼손, 선거, 플랫폼 운영자의 책임과 의무 등 딥페이크 관련 법적이슈와 관련된 법령을 살펴보았다. 위 내용은 딥페이크 사건의 가해자(제작자, 유포자 등), 피해자, 플랫폼 운영자의 책임 등 법적주체의 개별적 책임영역에 관한 것으로, 사전적·예방적인 조치가 아닌 사후적 조치에 관한 것이었다.

딥페이크 기술로 인한 순기능을 촉진시키고 역기능을 저하시키기 위하여는 정부의 선제적인 시책마련 등이 중요하며, 해외에서도 딥페이크 기술을 규제하기 위한 정부의 시책마련 등에 대한 법안이 마련되어 있다.

이하에서는 현행 법령 상 딥페이크 관련 정부 시책마련 등이 어떻게 규정되어 있는지 살펴본다.

나. 정보통신망 이용촉진 및 정보보호 등에 관한 법률

정보통신망법 제44조 제3항에서는 방송통신위원회는 정보통신망에 유통되는 정보로 인한 사생활 침해 또는 명예훼손 등 타인에 대한 권리침해를 방지하기 위하여 기술개발·교육·홍보 등에 대한 시책을 마련하고 이를 정보통신서비스 제공자에게 권고할 수 있다고 규정하고 있다. 딥페이크 영상이 사생활 침해 또는 명예훼손 등 타인에 권리침해를 유발하는 면이 있는바, 위 시책마련의 범위에는 딥페이크 영상에 관한 것도 포함된다고 볼 수 있다.

정보통신망 이용촉진 및 정보보호 등에 관한 법률

제44조(정보통신망에서의 권리보호)

- ① 이용자는 사생활 침해 또는 명예훼손 등 타인의 권리를 침해하는 정보를 정보통신망에 유통시켜서는 아니 된다.
- ② 정보통신서비스 제공자는 자신이 운영·관리하는 정보통신망에 제1항에 따른 정보가 유통되지 아니하도록 노력하여야 한다.
- ③ 방송통신위원회는 정보통신망에 유통되는 정보로 인한 사생활 침해 또는 명예훼손 등 타인에 대한 권리침해를 방지하기 위하여 기술개발·교육·홍보 등에 대한 시책을

마련하고 이를 정보통신서비스 제공자에게 권고할 수 있다.

그런데 최근 개정된 정보통신망법(2020. 6. 29. 공포, 2020. 12. 10. 시행)에서는 더욱 본격적으로 딥페이크 관련 내용을 담고 있다.

개정된 정보통신망법은 과학기술정보통신부장관 또는 방송통신위원회로 하여금 정보통신망을 통하여 유통되는 정보 중 인공지능 기술을 이용하여 만든 거짓의 음성·화상 또는 영상 등의 정보를 식별하는 기술의 개발·보급에 관한 시책을 마련할 것을 규정하고 있다(제4조 제1항, 제2항 제7의2호)⁸⁷⁾.

딥페이크 영상은 인공지능 기술을 이용하여 만든 거짓의 음성·화상 또는 영상 등의 정보에 해당하되, 딥페이크 영상 관련 시책마련에 관한 조항이라고 할 수 있다.

정보통신망 이용촉진 및 정보보호 등에 관한 법률

제4조(정보통신망 이용촉진 및 정보보호 등에 관한 시책의 마련)

① 과학기술정보통신부장관 또는 방송통신위원회는 정보통신망의 이용촉진 및 안정적 관리·운영과 이용자 보호 등(이하 "정보통신망 이용촉진 및 정보보호등"이라 한다)을 통하여 정보사회의 기반을 조성하기 위한 시책을 마련하여야 한다.

② 제1항에 따른 시책에는 다음 각 호의 사항이 포함되어야 한다.

1. 정보통신망에 관련된 기술의 개발·보급
2. 정보통신망의 표준화
3. 정보내용물 및 제11조에 따른 정보통신망 응용서비스의 개발 등 정보통신망의 이용 활성화
4. 정보통신망을 이용한 정보의 공동활용 촉진
5. 인터넷 이용의 활성화
6. 삭제<2020.2.4.>
- 6의2. 삭제<2020.2.4.>
7. 정보통신망에서의 청소년 보호

87) 참고로 중국 네트워크 오디오 및 비디오 정보 서비스 관리규정(网络音视频信息服务管理规定, Regulations on the Administration of Network Audio and Video Information Services)은 온라인 오디오·영상정보서비스 제공자로 하여금 오디오 및 비디오 정보 관리를 강화하고 불법, 그리고 가상 오디오 및 비디오 식별 기술을 배치 및 적용하여 이를 발견할 의무를 부과하고 있다(제12조).

7의2. 정보통신망을 통하여 유통되는 정보 중 인공지능 기술을 이용하여 만든 거짓의 음향·화상 또는 영상 등의 정보를 식별하는 기술의 개발·보급

8. 정보통신망의 안전성 및 신뢰성 제고

9. 그 밖에 정보통신망 이용촉진 및 정보보호등을 위하여 필요한 사항

다. 소결

위와 같이 최근 개정된 정보통신망법 제4조 제2항 제7의2호는 구체적으로 딥페이크라는 용어를 사용하고 있지는 아니하나, 정보통신망을 통하여 유통되는 정보 중 인공지능 기술을 이용하여 만든 거짓의 음향·화상 또는 영상 등의 정보를 식별하는 기술의 개발·보급이라고 하여, 딥페이크 식별 기술의 개발·보급을 위한 시책마련을 규정하고 있다.

딥페이크 생성 기술에 대한 원동력이 더욱 강하고, 딥페이크 식별 기술에 대한 요구는 많지 않은 현실에서, 정부에서 딥페이크 식별 기술의 발전과 보급을 위한 시책을 마련하도록 규정하는 것이 필요한바, 정보통신망법 제4조 제2항 제7의2호의 마련으로 기존의 입법공백이 해소된 것으로 보인다.

10. 결어

이상에서, 음란물, 명예훼손, 퍼블리시티권, 초상권 침해, 보이스피싱, 피해자의 삭제, 처리정지 등 조치요구, 정보통신서비스 제공자의 의무와 책임, 선거 등 딥페이크 이슈와 관련 법령을 검토하였다. 각 법적이슈와 관련된 관련법령은 아래와 같다.

<표 3-3> 딥페이크 관련 이슈와 국내 관련 법령

법적이슈		관련법령	개선논의
1	음란물	성폭력처벌법 제14조의2(허위영상물 등의 반포등), 제15조(미수범)	○ (개선논의) 성폭력처벌법 제14조의2 제1항 목적조항의 삭제

			여부 ○ (규정신설검토) 소지 행위에 대한 처벌규정 검토
		정보통신망법 제44조의7(불법정보의 유통금지 등) 제1항 제1호, 제74조 (벌칙) 제1항 제2호	
2	명예훼손 · 사자명예 훼손	형법 제307조(명예훼손), 제309조(출 판물등에 의한 명예훼손)	
		정보통신망법 제70조(벌칙), 제44조 의7(불법정보의 유통금지 등)	
		형법 제308조(사자의 명예훼손)	
3	퍼블리시 티권·초 상권 침해	판례, 학설 등에 의하여 인정되는 권리	
4	저작권	저작권법 제136조 제1항 제1호	
5	보이스피 싱	통신사기피해환급법 제15조의 2(벌 칙)	
6	선거	공직선거법 제110조(후보자 등의 비 방금지), 제250조(허위사실공표죄)	○ (개선논의) 해외에서는 선거 관련하여 딥페이크 영상에 관한 논의가 활발하며 선거일을 기준 으로 하여 구체적인 처벌규정을 마련하고 있는바, 현행 공직선거 법 상 개선점이 있는지 검토할 필요가 있음
7	피해자의 삭제· 처리정지 등 조치요구	개인정보보호법 제36조(개인정보의 정정·삭제), 제37조(개인정보의 처 리정지 등)	
		정보통신망법 제44조의2(정보의 삭제 요청 등)	
		성폭력처벌법 일부개정법률안 제31 조 제3항	
8	플랫폼 운영자의 책임과	정보통신망법 제44조(정보통신망에서 의 권리보호)	
		정보통신망법 제44조의2(정보의 삭제	

	의무	요청 등), 제44조의3(임의의 임시조치)	
		정보통신망법 제44조의7(불법정보의 유통금지 등)	○ (입법공백) 정보통신망법 제44조의7 제3항 제1호에 성폭력 처벌법 제14조의2 포함여부 검토
		정보통신망법 제44조의9(불법촬영물 등 유통방지 책임자), 제76조(과태료) 제2항	
		정보통신망법 제64조의5(투명성 보고서 제출의무 등), 제76조(과태료) 제3항	
		전기통신사업법 제22조의5(부가통신사업자의 불법촬영물 등 유통방지)	
9	정부시책 마련	정보통신망법 제4조(정보통신망 이용 촉진 및 정보보호등에 관한 시책의 마련) 제1,2항, 제44조(정보통신망에서의 권리보호) 제3항	

현재 국내에서는 딥페이크 관련하여 단독으로 법률안이 발의한 된 것은 없으나, 이미 현행 법률만으로 딥페이크 관련 법적이슈가 상당부분 해결되고 있으며, 결정적인 입법적인 공백은 발견되지 아니한다.

딥페이크만을 다룬 단독 법률안이 발의되는 경우 딥페이크를 정면으로 정의내릴 가능성이 높다. 그러나 딥페이크 기술 이외에 향후 인공지능을 기반으로 한 새로운 기술의 출현까지 포괄하기 위하여는 넓은 의미의 기술로 정의하는 것이 바람직하다. 최근 개정된 정보통신망법은 '정보통신망을 통하여 유통되는 정보 중 인공지능 기술을 이용하여 만든 거짓의 음향·화상 또는 영상 등의 정보를 식별하는 기술의 개발·보급'에 관한 시책을 마련할 것을 규정하고 있는바(제4조 제1항, 제2항 제7의2호), 제7조의2호에 정의된 기술은 딥페이크 기술을 포괄하는 것으로서 옳은 방향으로 입법된 것으로 보인다. 추후 신설 또는 개정될 법률은 정보통신망법 제4조 제2항 제7의2호의 내용을 참조할 수 있다.

위와 같이 국내 법령 상 이미 기존 법률로서 딥페이크 관련 법적이슈가 해결되고 있으나, 다만 성폭력처벌법 제14조의2(허위영상물 등의 반포등) 제1항 상 목적조항의 삭제 또는 유지여부, 성폭력처벌법 제14조의2 내 소지행위 처벌규정 신설여부가 검토되어야 할 것으로 보이며, 해외에서 딥페이크 관련 논의가 선거법 쪽에서 활발하게 일어나고 있는 것에 비하여 국내에서는 아직까지 이렇다 할 개정작업이 진행되지 않고 있어, 해외 사례에 비추어 국내 공직선거법을 개선하여야 할지에 대한 추가적인 검토가 필요해 보인다.

이하에서는 성폭력처벌법, 정보통신망법, 공직선거법 상 법적이슈별로 입법 개선논의가 필요한 사항에 관하여 검토하도록 한다.

제3절 딥페이크 관련 법적이슈와 국내 입법개선 논의

1. 성폭력범죄의 처벌 등에 관한 특례법

가. 서설

최근 딥페이크 기술로 제작한 음란영상물을 규제하기 위한 성폭력처벌법 제14조의2가 신설되었다. 그러나 제14조의2 제1항은 반포등의 목적없이 제작된 딥페이크 영상의 경우 처벌이 어려운 문제점이 있어 목적조항의 삭제여부를 검토할 필요성이 있으며, 동법 제14조와는 달리 허위 음란영상물을 반포하지 아니하고 소지만한 경우에 대하여는 처벌규정이 없어 이에 대한 규정신설을 검토할 필요성이 있다.

나. 성폭력처벌법 제14조의2 제1항 목적조항 삭제여부

성폭력처벌법 제14조의2(허위영상물 등의 반포등) 제1항은 반포등(반포·판매·임대·제공 또는 공공연하게 전시·상영⁸⁸⁾)의 '목적'으로 사람의 얼굴·신체 또는 음성을 대상으로 한 촬영물·영상물 또는 음성물(이하 이 조에서 "영상물등"이라 한다)을 영상물등의 대상자의 의사에 반하여 성적 욕망 또는 수치심을 유발할 수 있는 형태로 편집·합성 또는 가공(이하 이 조에서 "편집등"이라 한다)한 자는 5년 이하의 징역 또는 5천만원 이하의 벌금에 처한다고 규정하고 있다.

성폭력범죄의 처벌 등에 관한 특례법

제14조의2(허위영상물 등의 반포등)

① 반포등을 할 목적으로 사람의 얼굴·신체 또는 음성을 대상으로 한 촬영물·영상물 또는 음성물(이하 이 조에서 "영상물등"이라 한다)을 영상물등의 대상자의 의사에 반하여 성적 욕망 또는 수치심을 유발할 수 있는 형태로 편집·합성 또는 가공(이하 이 조에서 "편집등"이라 한다)한 자는 5년 이하의 징역 또는 5천만원 이하의 벌금에

88) 성폭력처벌법 제14조 제2항의 '반포 등' 정의에 의한다.

처한다.

② 제1항에 따른 편집물·합성물·가공물(이하 이 항에서 "편집물등"이라 한다) 또는 복제물(복제물의 복제물을 포함한다. 이하 이 항에서 같다)을 반포등을 한 자 또는 제1항의 편집등을 할 당시에는 영상물등의 대상자의 의사에 반하지 아니한 경우에도 사후에 그 편집물등 또는 복제물을 영상물등의 대상자의 의사에 반하여 반포등을 한 자는 5년 이하의 징역 또는 5천만원 이하의 벌금에 처한다.

그러나 제14조의2의 참조규정인 제14조 제1항은 카메라나 그 밖에 이와 유사한 기능을 갖춘 기계장치를 이용하여 성적 욕망 또는 수치심을 유발할 수 있는 사람의 신체를 촬영대상자의 의사에 반하여 촬영한 자는 7년 이하의 징역 또는 5천만원 이하의 벌금에 처한다고 하여, 반포등의 목적을 요구하지 않고 있다.

성폭력처벌법 제14조의2 제1항이 반포등의 목적을 요구함으로 인하여, 반포등(반포·판매·임대·제공 또는 공공연하게 전시·상영)의 '목적 없이' 사람의 얼굴·신체 또는 음성을 대상으로 한 촬영물·영상물 또는 음성물(이하 이 조에서 "영상물등"이라 한다)을 영상물등의 대상자의 의사에 반하여 성적 욕망 또는 수치심을 유발할 수 있는 형태로 편집·합성 또는 가공(이하 이 조에서 "편집등"이라 한다)한 자에 대하여는 처벌이 불가능하다.

형사처벌 조항에서 목적을 요구하고 있는 경우 그 목적의 존재에 대한 입증책임은 수사기관이 부담하는바, 만약 수사기관이 딥페이크 기술을 이용한 음란영상물의 편집·합성·가공 당시 반포·판매·임대·제공 또는 공공연하게 전시·상영할 목적이 있었음을 입증하지 못한다면 딥페이크 음란영상물의 제작자를 처벌하게 못하게 된다.

딥페이크 기술을 이용한 음란영상물은 주로 유명인을 대상으로 제작되고 있으며, 그로 인한 파급효과가 워낙 크기 때문에 이를 유통시키면 막대한 이익을 얻을 수 있다. 이 때문에 유명인을 대상으로 한 딥페이크 음란영상물은 불법적으로 유통하여 영리를 취할 목적으로 계획적으로 편집·합성·가공되는 경우가 많다⁸⁹⁾.

89) 2020. 4. 21.자 이데일리 기사 - '女연예인 얼굴 합성' 딥페이크 음란물 유포.. 수사 中 <https://www.edaily.co.kr/news/read?newsId=01498966625738416&mediaCodeNo=257&OutLnkChk=Y>

그러나 반포등의 목적이 없는 상태에서 제작된 딥페이크 음란영상물이라도 추후 얼마든지 반포·판매·임대·제공·전시·상영될 가능성이 있으며, 딥페이크 영상은 육안으로서는 허위인지 여부를 판명하기 어려운바 반포등 목적없이 제작된 딥페이크 음란영상물로 인한 피해는 반포등을 목적으로 제작된 딥페이크 음란영상물과 아무런 차이가 없다. 따라서 애초부터 당사자의 의사에 반해 딥페이크 기술을 이용한 음란영상물을 만드는 것을 규제할 필요성이 있다.

입법 당시 성폭력처벌법 제14조의2 일부개정법률안의 제안경위를 보더라도⁹⁰⁾, '특정 인물의 신체 등을 대상으로 한 영상물등을 성적 욕망 또는 수치심을 유발할 수 있는 형태로 편집하는 등의 소위 딥페이크를 제작·반포하는 행위 등에 대한 국민적 처벌 요구가 강함. 그러나, 딥페이크 제작 등의 기술이 빠르게 발전함에도 불구하고, 현행 규정으로는 그 처벌에 한계가 있거나 처벌이 미약하여 이에 대한 별도의 처벌 규정을 마련할 필요성이 증가하고 있음. 이에 사람의 신체 등을 대상으로 한 영상물등을 대상자의 의사에 반하여 성적 욕망 또는 수치심을 유발할 수 있는 형태로 편집 또는 반포 등의 행위를 한 자에 대한 처벌 규정을 마련함과 동시에 영리목적으로 정보통신망을 이용하여 반포 등을 한 경우 가중처벌하려는 것임(안 제14조의2 신설)'이라고 하여, 특별히 목적조항의 추가여부를 논의하지 않고 있다.

해외에서도 딥페이크 음란영상물의 제작 및 유포를 형사처벌하고 있으나, 딥페이크 영상 제작시의 반포등의 목적을 요구하는 사례는 발견되지 아니한다.

90) 성폭력처벌법 일부개정법률안(대안) 원안, 의안번호 : 24689, 제안연월일 : 2020. 3. 제안자 : 법제사법위원장

<표 3-4> 딥페이크 기술로 제작된 음란영상물에 대한 해외 입법례

구 분	내 용	비 고
2019년 책임법에 따라 부당한 이용으로부터 유래한 허위의 외관으로부터 모든 사람들을 보호하기 위한 법률 ⁹¹⁾ / 미국 연방법률	거짓으로 등장하는 사람을 모욕하거나 다른 방법으로 괴롭히려는 의도를 가지고 첨단 기술 허위 개인화 기록(an advanced technological false personation record)에 성적인 내용이 포함되어 있고 성행위를 하거나 나체 상태에 있는 사람이 등장하도록 한 경우 형사처벌함	입법진행중
프라이버시권 및 퍼블리시티권에 관한 민권법을 개정하고, 퍼블리시티권 침해 조치 개시의 적시성에 관한 민사관행법 및 규칙을 개정하는 법안 ⁹²⁾ / 미국 뉴욕주	개인의 동의 없이, 그 개인이 수행하고 있다는 인상을 주는 방식으로 음란물에 Digital replica를 사용하는 경우 법 위반으로 간주함(\$ 51의 4). 피해자는 법 위반자에 대하여 손해배상을 청구할 수 있음(\$ 51의 6.)	현재시행
타인 이미지의 불법 배포 또는 판매에 관한 법 ⁹³⁾ / 미국 버지니아주	허위로 만든 포르노 비디오 및 사진을 유포하는 경우 1급 경범죄에 해당하도록 함으로서 딥페이크 기술을 사용한 비디오 및 사진 등이 성적인 내용을 포함할시 해당 비디오 및 사진을 만들어낸 사람을 처벌할 수 있도록 함(Va Code Ann. §18.2-386.2, A.)	현재시행
AB-602 디지털 또는 전자 기술을 이용한 개인 묘사: 성적으로 노골적인 소재: 청구원인 법 / 미국 캘리포니아주	캘리포니아주 주민들이 그들의 사진이나 영상이 성적으로 노골적인 콘텐츠에 악용될 경우 소송을 제기할 수 있도록 함(SECTION 1. 1708.86.(e))	현재시행
주 형법 내 사이버스토킹 법 ⁹⁴⁾ / 미국 미시건주	피해자가 공포, 겁, 협박, 위협, 회롱 또는 성희롱을 느끼게 하는 행동을 유발하기 위한 메시지를 피해자의 동의 없이 인터넷 등 게시하는 행위를 형사처벌함(제750.411s조 (1))	현재시행
형법 ⁹⁵⁾ / 호주 뉴사우스웨일즈주	딥페이크 영상 등 조작된 영상이 특정인을 나타내며 동의 없이 성적인 개인 이미지를 촬영 또는 유포하는 경우 형사처벌함(91N, 91P, 91Q)	현재시행

91) Defending Each and Every Person from False Appearances by Keeping Exploitation Subject to Accountability Act of 2019

이상과 같이 성폭력처벌법 제14조의2 제1항을 신설하면서 제14조와 달리 목적조항을 포함시킴으로써, 반포등 목적없이 제작된 딥페이크 음란영상물의 경우에는 처벌할 수 없는 문제점이 있는바, 목적조항을 삭제하는 것이 바람직하다.

다. 딥페이크 음란물 소지 행위에 대한 처벌규정 신설여부

성폭력처벌법 제14조의2(허위영상물 등의 반포등)은 동법 제14조(카메라 등을 이용한 촬영)를 참조로 하여 신설되었다.

성폭력처벌법 제14조 제4항에서는 (제14조) 제1항 또는 제2항의 촬영물 또는 복제물을 소지·구입·저장 또는 시청한 자는 3년 이하의 징역 또는 3천만원 이하의 벌금에 처한다고 하여, 카메라 등 이용 촬영죄로 인하여 생성된 음란물의 소지·구입·저장·시청을 처벌하고 있다. 위 규정은 최근 개정되어 2020. 5. 19.부터 시행되었다.

성폭력범죄의 처벌 등에 관한 특례법

제14조(카메라 등을 이용한 촬영)

- ① 카메라나 그 밖에 이와 유사한 기능을 갖춘 기계장치를 이용하여 성적 욕망 또는 수치심을 유발할 수 있는 사람의 신체를 촬영대상자의 의사에 반하여 촬영한 자는 7년 이하의 징역 또는 5천만원 이하의 벌금에 처한다.
- ② 제1항에 따른 촬영물 또는 복제물(복제물의 복제물을 포함한다. 이하 이 조에서 같다)을 반포·판매·임대·제공 또는 공공연하게 전시·상영(이하 "반포등"이라 한다)한 자 또는 제1항의 촬영이 촬영 당시에는 촬영대상자의 의사에 반하지 아니한 경우(자신의 신체를 직접 촬영한 경우를 포함한다)에도 사후에 그 촬영물 또는 복제물을 촬영대상자의 의사에 반하여 반포등을 한 자는 7년 이하의 징역 또는 5천만원 이하의 벌금에 처한다.

92) An act to amend the civil rights law, in relation to the right of privacy and the right of publicity; and to amend the civil practice law and rules, in relation to the timeliness of commencement of an action for violation of the right of publicity

93) Unlawful Dissemination or Sale of Images of Another Person

94) The Michigan Penal Code (Excerpt)Act 328 of 1931, 750.411s

95) Crimes Act 1900

④ 제1항 또는 제2항의 촬영물 또는 복제물을 소지·구입·저장 또는 시청한 자는 3년 이하의 징역 또는 3천만원 이하의 벌금에 처한다.

한편, 음란물의 소지죄를 처벌하는 규정은 성폭력처벌법 제14조 제4항 이외에도, 아동·청소년의 성보호에 관한 법률 제11조 제5항이 있다. 아동·청소년의 성보호에 관한 법률 제11조 제5항은 아동·청소년성착취물을 구입하거나 아동·청소년성착취물임을 알면서 이를 소지·시청한 자는 1년 이상의 징역에 처한다고 규정하고 있다.

아동·청소년의 성보호에 관한 법률

제11조(아동·청소년성착취물의 제작·배포 등)

- ① 아동·청소년성착취물을 제작·수입 또는 수출한 자는 무기징역 또는 5년 이상의 유기징역에 처한다.
- ② 영리를 목적으로 아동·청소년성착취물을 판매·대여·배포·제공하거나 이를 목적으로 소지·운반·광고·소개하거나 공연히 전시 또는 상영한 자는 5년 이상의 징역에 처한다.
- ③ 아동·청소년성착취물을 배포·제공하거나 이를 목적으로 광고·소개하거나 공연히 전시 또는 상영한 자는 3년 이상의 징역에 처한다.
- ④ 아동·청소년성착취물을 제작할 것이라는 정황을 알면서 아동·청소년을 아동·청소년성착취물의 제작자에게 알선한 자는 3년 이상의 징역에 처한다.
- ⑤ 아동·청소년성착취물을 구입하거나 아동·청소년성착취물임을 알면서 이를 소지·시청한 자는 1년 이상의 징역에 처한다.
- ⑥ 제1항의 미수범은 처벌한다
- ⑦ 상습적으로 제1항의 죄를 범한 자는 그 죄에 대하여 정하는 형의 2분의 1까지 가중한다.

그러나 성폭력처벌법 제14조의2에는 소지·구입·저장·시청을 처벌하는 규정이 없다.

성폭력처벌법 제14조 제4항 제안이유를 보면⁹⁶⁾, '사이버 성범죄로 인한 피해가 날로 증가하고 있는 상황에서 최근 텔레그램을 이용한 성착취 사건으로 인해 국민적 관심사가 매우 고조된 상황임. 국회 국민동의청원 홈페이지에서도 텔레그램 n번방 사건을

96) 성폭력처벌법 일부개정법률안(대안), 의안번호 : 24883, 제안연월일 : 2020. 4, 제안자 : 법제사법위원회

비슷한 사이버 성범죄의 처벌법 제정에 관한 청원이 10만명의 동의를 얻어 현재 국회에 계류되어 있음. 이에 카메라 등 이용 촬영죄 등 성폭력범죄의 법정형을 상향하고, 불법 성적 촬영물의 소지·구입·저장·시청에 대한 처벌규정을 신설하는 등 관련 규정을 정비함으로써 사이버 성범죄로 인한 피해 발생을 미연에 방지하여 국민의 성적 자기결정권 등 기본권을 보호하고 범죄로부터 안전한 사회 조성에 기여하려는 것임.'이라고 되어 있는바, n번방 사건과 같은 사이버 성범죄를 방지하려는 목적을 가지고 있다.

딥페이크 기술로 제작한 음란영상물의 경우 n번방 사건의 성착취물과 마찬가지로, 텔레그램 등 메신저를 통하여 유통되고 있고, 딥페이크는 기존 음란물에 얼굴만을 합성하면 되기 때문에 그 음란물의 수위 또한 심각한 수준이다⁹⁷⁾.

성폭력처벌법 제14조 제1항과 제14조의2 제1항은 전부 대상자의 의사에 반하여 촬영되거나 제작되었을 것을 기본 요건으로 하고 있고, 제14조 및 제14조의2의 영상물은 전부 텔레그램 등 온라인을 통하여 유포되며, 영상물을 보는 사람이 다운로드 등 같은 방법으로 해당 음란물을 소지·구입·저장·시청한다는 점이 동일하다. 그럼에도 불구하고 제14조에 의한 영상물의 소지등은 처벌되고, 제14조의2에 의한 영상물의 소지등은 처벌되지 아니한다는 것은 입법적인 불균형이 있는 것으로 보인다.

위와 같은 사정을 종합할 때, 사이버 성범죄의 근절을 위하여 성폭력처벌법 제14조의2에도 마찬가지로 소지·구입·저장·시청에 대한 처벌규정을 신설하는 것이 바람직하다⁹⁸⁾.

라. 소결

97) 2020. 3. 27.자 한국경제 기사 - 회원 2000명 우르르...女 아이돌 딥페이크 텔레그램방 '충격'

<https://www.hankyung.com/society/article/202003275942H>

98) 다만, 해외 입법례에서는 딥페이크 기술로 제작된 음란영상물의 소지·구입·저장·시청에 대한 별도의 형사처벌 조항은 발견되지 아니한다.

위와 같이 성폭력처벌법 제14조의2 제1항에서 규정하고 있는 반포등의 목적 조항을 삭제함으로써, 반포등 목적없이 딥페이크 기술을 이용하여 음란영상물을 제작한 경우에도 처벌할 수 있게 하는 것이 바람직하다.

또한 성폭력처벌법 제14조 제4항과 균형을 맞추어 제14조의2에도 딥페이크 기술을 이용한 음란영상물의 소지·구입·저장·시청 행위에 대한 형사처벌규정을 신설하는 것이 바람직하다.

2. 정보통신망 이용촉진 및 정보보호 등에 관한 법률

정보통신망법 제44조의7 제1항은 누구든지 제1항 각 호의 어느 하나의 해당하는 정보를 유통하여서는 아니된다고 하면서, 제9호에서 그 밖의 범죄를 목적으로 하거나 교사 또는 방조하는 내용의 정보를 규정하고 있다.

정보통신망법 제44조의7 제3항에서는 방송통신위원회가 제44조의7 제1항 제9호의 정보가 제3항 각 호의 요건 모두에 해당하는 경우에는 정보통신서비스 제공자 또는 게시관 관리·운영자에게 해당 정보의 처리를 거부·정지 또는 제한하도록 명하여야 한다고 규정하고 있다. 정보통신망법 제44조의7 제3항 제1호는 관계 중앙행정기관의 장의 요청[제1항제9호의 정보 중 성폭력범죄의 처벌 등에 관한 특례법 제14조에 따른 촬영물 또는 복제물(복제물의 복제물을 포함한다)에 대하여는 수사기관의 장의 요청을 포함한다]이 있었을 것을 요건으로 한다.

정보통신망 이용촉진 및 정보보호 등에 관한 법률

제44조의7(불법정보의 유통금지 등)

① 누구든지 정보통신망을 통하여 다음 각 호의 어느 하나에 해당하는 정보를 유통하여서는 아니 된다.

7. 법령에 따라 분류된 비밀 등 국가기밀을 누설하는 내용의 정보

8. 「국가보안법」에서 금지하는 행위를 수행하는 내용의 정보

9. 그 밖에 범죄를 목적으로 하거나 교사(敎唆) 또는 방조하는 내용의 정보

③ 방송통신위원회는 제1항제7호부터 제9호까지의 정보가 다음 각 호의 모두에 해당

하는 경우에는 정보통신서비스 제공자 또는 게시판 관리·운영자에게 해당 정보의 처리를 거부·정지 또는 제한하도록 명하여야 한다.

1. 관계 중앙행정기관의 장의 요청[제1항제9호의 정보 중 「성폭력범죄의 처벌 등에 관한 특례법」 제14조에 따른 촬영물 또는 복제물(복제물의 복제물을 포함한다)에 대하여는 수사기관의 장의 요청을 포함한다]이 있었을 것
2. 제1호의 요청을 받은 날부터 7일 이내에 심의위원회의 심의를 거친 후 「방송통신위원회의 설치 및 운영에 관한 법률」 제21조제4호에 따른 시정 요구를 하였을 것
3. 정보통신서비스 제공자나 게시판 관리·운영자가 시정 요구에 따르지 아니하였을 것

딤페이크 영상은 정보통신망법 제44조의7 제1항 제9호 그 밖의 범죄를 목적으로 하거나 교사 또는 방조하는 내용의 정보에 해당할 수 있고, 제44조의7 제3항 제1호에 비추어 제44조의7 제1항 제9호의 정보에는 성폭력처벌법 제14조의 음란영상물이 포함될 것이 예정되어 있는 것으로 보인다.

그럼에도 불구하고 제44조의7 제3항 제1호에 성폭력처벌법 제14조의2가 포함되어 있지 아니한바, 이는 최근 신설된 성폭력처벌법 제14조의2가 미처 반영되지 못한 입법공백으로 볼 여지가 높다. 제14조와 제14조의2를 차별해야 할 특별한 이유가 없기 때문이다. 정보통신망법 제44조의7 제3항 제1호에 성폭력처벌법 제14조 이외 제14조의2 추가를 고려하여야 할 것으로 보인다.

3. 공직선거법

가. 서설

공직선거법 제110조(후보자 등의 비방금지) 및 제250조(허위사실공표죄)에서는 선거운동을 위하여 공연히 허위사실을 적시하거나 당선되거나 되지 않게 할 목적으로 허위의 사실을 공표하지 못하도록 하고 있는바, 선거 관련 허위정보를 담은 딤페이크 영상 또한 위 규정에 의하여 규제가 가능하다.

해외에서는 선거와 관련된 입법 및 개정 논의가 활발한바, 해외 입법례에 비추어 국내 공직선거법 상 개선점이 있는지 검토할 필요가 있다.

나. 해외 입법례 검토

공직선거법 제110조(후보자 등의 비방금지) 및 제250조(허위사실공표죄)는 다음과 같이 선거운동을 위한 공연한 허위사실 적시, 당선되거나 되지 않게 할 목적으로 한 허위의 사실의 공표를 금지하고 있다. 현행 공직선거법 상 허위사실 적시 및 허위사실공표의 수단에 관하여는 별도로 언급하고 있는 조항은 없다.

공직선거법

제110조(후보자 등의 비방금지)

① 누구든지 선거운동을 위하여 후보자, 배우자 또는 직계존비속이나 형제자매의 출생지·가족관계·신분·직업·경력등·재산·행위·소속단체, 특정인 또는 특정단체로부터의 지지여부 등에 관하여 허위의 사실을 공표할 수 없으며, 공연히 사실을 적시하여 사생활을 비방할 수 없다. 다만, 진실한 사실로서 공공의 이익에 관한 때에는 그러하지 아니하다.

제250조(허위사실공표죄)

① 당선되거나 되게 할 목적으로 연설·방송·신문·통신·잡지·벽보·선전문서 기타의 방법으로 후보자에게 유리하도록 후보자, 후보자의 배우자 또는 직계존비속이나 형제자매의 출생지·가족관계·신분·직업·경력등·재산·행위·소속단체, 특정인 또는 특정단체로부터의 지지여부 등에 관하여 허위의 사실[학력을 게재하는 경우 제64조제1항의 규정에 의한 방법으로 게재하지 아니한 경우를 포함한다]을 공표하거나 공표하게 한 자와 허위의 사실을 게재한 선전문서를 배포할 목적으로 소지한 자는 5년이하의 징역 또는 3천만원이하의 벌금에 처한다.

② 당선되지 못하게 할 목적으로 연설·방송·신문·통신·잡지·벽보·선전문서 기타의 방법으로 후보자에게 불리하도록 후보자, 그의 배우자 또는 직계존·비속이나 형제자매에 관하여 허위의 사실을 공표하거나 공표하게 한 자와 허위의 사실을 게재한 선전문서를 배포할 목적으로 소지한 자는 7년 이하의 징역 또는 500만원 이상 3천만원 이하의 벌금에 처한다.

선거와 관련된 딥페이크 영상에 관한 해외 입법례는 아래와 같다.

<표 3-5> 딥페이크 기술로 제작된 영상과 선거에 관한 해외 입법례

구 분	내 용
선거 결과에 영향을 미치려는 의도로 기만적 동영상 조작한 범죄와 관련한 법 ⁹⁹⁾ / 미국 텍사스주	선거 후보자에게 영향을 미칠 의도로 (1) 딥페이크 비디오를 제작하는 경우, (2) 딥페이크 동영상이 선거일 전 30일 이내에 게시 또는 배포되도록 하는 경우 형사처벌함(SEC. 255.004. (d)-(2))
AB-730 선거: 기만적인 오디오 또는 시각적 미디어 법 ¹⁰⁰⁾ / 미국 캘리포니아 주	선거일(투표일) 기준 60일 이내에 특정 후보를 대상으로 악의적으로 조작 또는 변조한 동영상, 이미지 또는 오디오를 제작하거나 배포하는 행위로 선거 결과에 영향을 미치는 것을 금지함(SEC.4. 20010.(a)). 영상이 가짜로 제작된 것을 명시하는 경우에는 적용제외(SEC.4. 20010.(d)(4)).
선거법-온라인 캠페인 자료 - 딥페이크 사용 ¹⁰¹⁾ / 미국 메릴랜드 주 (기간만료로 폐기)	선거일(투표일)로부터 90일 이전에 온라인에 딥페이크를 게시, 배포함으로써 유권자들이 특정 후보에 대하여 투표하는 것에 고의로 영향을 미치거나 미치려는 것을 금지함(13-401.1(C)(1)). 오디오 녹음, 비디오 녹화 또는 사진의 내용이 변경되었다는 정보 등 딥페이크에 대한 특정 정보를 명확하고 눈에 띄는 방식으로 공개한 경우에는 적용제외(13-401.1(C)(2)).
선거법 ¹⁰²⁾ / 프랑스	선거기간 동안 특정 사실에 대해 부정확하거나 오해소지가 있는 주장이 온라인 공공정보 통신서비스를 통해 고의 또는 자동적으로 대량 유포되는 경우, 가처분 전담판사는 검찰, 후보자, 정당, 정치집단 등의 요청에 따라 해당 정보의 유포를 중단시키기 위한 조치를 취하도록 명할 수 있음(Article L163-2).

99) Relating to the creation of a criminal offense for fabricating a deceptive video with intent to influence the outcome of an election

100) AB-730 Elections: deceptive audio or visual media

101) Election Law - Online Campaign Material - Use of Deepfakes

102) Code électoral, 정보조작 대처에 관한 2018. 12. 22. 법률 제2018-1202호 정보조작대처법(LOI n° 2018-1202 du 22 decembre 2018 relative a la lutte contre la manipulation de l'information)에 의하여 개정됨

미국에서 가장 활발하게 딥페이크 영상과 선거에 관한 논의가 이루어지고 있으며 이미 여러 주에서 관련 선거법을 시행하고 있다. 텍사스주에서는 선거후보자에게 영향을 미칠 의도로 딥페이크 영상을 제작하지만 해도 처벌하고 있으며, 캘리포니아주에서는 선거일 기준 60일 이내에 특정 후보를 대상으로 악의적으로 조작 또는 변조한 동영상, 이미지 또는 오디오를 제작하거나 배포함으로써 선거 결과에 영향을 미치는 행위를 금지한다. 또한 메릴랜드주¹⁰³⁾에서는 선거일 기준 90일 이전에 딥페이크 영상을 게시, 배포함으로써 선거에 영향을 미치려는 행위를 금지하고 있다. 다만 캘리포니아주와 메릴랜드주는 해당 영상이 가짜로 제작된 것임을 명시한 경우에는 적용을 제외한다.

현행 공직선거법은 선거에 영향을 미치려는 의도로 딥페이크 영상을 제작, 배포하거나, 딥페이크 영상을 제작하거나 배포함으로써 선거에 영향을 미치는 행위에 관한 별도의 규정이 없다. 따라서 선거에 영향을 미치려는 목적으로 딥페이크 영상을 제작, 배포하거나, 딥페이크 영상을 제작, 배포함으로써 결과적으로 선거에 영향을 미치는 행위에 대한 처벌규정의 신설을 고려할 필요가 있다.

구체적으로, ㉠ 당선되거나 당선되지 못하게 할 목적으로 특정 후보자의 얼굴·신체 또는 음성을 대상으로 한 촬영물·영상물 또는 음성물을 편집·합성 또는 가공하여 유포하는 행위 자체를 처벌하는 조항, ㉡ 특정 후보자의 얼굴·신체 또는 음성을 대상으로 한 촬영물·영상물 또는 음성물을 편집·합성 또는 가공하여 유포함으로써 특정 후보자를 당선되거나 당선되지 못하게 한 행위를 처벌하는 조항을 신설하고, 딥페이크 영상을 통해 허위사실을 공표하는 행위는 기존 공직선거법 제250조를 통해 처벌함으로써, 딥페이크 기술 활용 허위 영상 등에 대한 처벌 공백을 해결하는 방향으로 공직선거법을 개정하는 안을 검토할 필요가 있다.

한편, 프랑스에서는 선거기간 동안 부정확한 정보가 유포되는 경우 이를 중단시키기 위한 조치를 취할 수 있다고 규정하고 있으나, 국내 법령상 선거기간을 불문하고 언제든지 허위정보에 대한 배포금지 가처분 등을 신청할 수 있으므로, 추가적인 입법

103) 해당 법안은 현재 기간만료로 폐기되었다.

은 필요하지 않은 것으로 보인다.

다. 소결

공직선거법에는 딥페이크 영상의 제작 또는 배포로 인해 선거에 영향을 주는 행위에 관한 별도의 처벌규정이 없으나, 선제적으로 공직선거법에 딥페이크 영상 관련 조항을 신설함으로써 딥페이크 영상이 선거에 영향을 미치는 것을 방지할 필요성이 있다.

4. 결어

이상에서 성폭력처벌법, 정보통신망법, 공직선거법 상 법적이슈별로 입법적으로 개선할 부분이 있는지 검토하였다.

성폭력처벌법 제14조의2 제1항의 목적조항 삭제와 제14조의2 내 소지조항의 신설은 사이버 성범죄 근절이라는 입법적 필요성이 있고, 제14조와의 균형 상 입법개선이 필요한 것으로 보인다. 또한 정보통신망법 제44조의7 제3항 제1호에는 성폭력처벌법 제14조만 포함되어 있고, 제14조의2가 포함되어 있지 아니한바, 이는 입법의 공백으로 보이는바 개선이 이루어져야 할 것으로 보인다.

나아가 현행 공직선거법에 허위사실적시, 허위사실공표에 관한 규정이 이미 존재하고 있기는 하나, 미국 등 해외 입법례에서 딥페이크 영상의 제작 또는 배포행위로 선거에 영향을 미치는 경우에 대한 별도의 조항을 신설하고 있고, 단순 허위사실적시 또는 허위사실공표에 비하여 딥페이크 영상의 제작 또는 배포로 인한 불법성이 더욱 크고 국민들에게 미치는 영향 또한 지대한바, 선제적으로 딥페이크 영상의 제작 또는 배포로 인해 선거에 영향을 미치는 행위에 대한 별도 조항을 신설하는 것이 바람직하다.

이하에서는 현재 딥페이크와 관련된 제도 현황을 살펴보고, 딥페이크 식별기술 도

입, 딥페이크 식별시 즉시삭제요구권 도입, 딥페이크 기술로 제작된 영상에 대한 표시 의무, 워터마크 삽입의무, 딥페이크 인증 등 전달기구 운영, 딥페이크 유통신고허가제, 국내대리인제도를 통해 피해자의 조치요구를 해외사업자에 확대할 수 있을지 여부 등 딥페이크와 관련된 정책 및 제도의 도입가능성에 관하여 검토하고자 한다.

제4장 딥페이크 기술 관련 국내 제도 현황 및 개선논의

제1절 서설

앞서, 제1장 제1절 연구의 배경 및 필요성 목차에서 전술한 바와 같이, 딥페이크 기술을 활용한 영상은 음란물 제작, 가짜뉴스 생산, 명예훼손 등 범죄에 악용될 가능성을 내포하고 있다. 그러나 최근 딥페이크 탐지 기술의 발전 속도가 딥페이크 기술의 발전 속도를 따라잡지 못하고 있는 추세에 비추어, 그 악용가능성을 기술적 수단으로 완전히 막아내기는 어려울 것이라는 비관론이 유력하게 제기되고 있다¹⁰⁴⁾.

기술적 수단에 의한 딥페이크의 탐지 또는 식별에 명확한 한계가 예상되는 이상, 이에 대한 정책적 차원에서의 대응책 마련이 불가피한 것으로 보인다. 즉, 딥페이크 영상물의 생성, 유통 각 단계에서의 규제체계의 신설 또는 보완 필요성이 대두된다. 규제체계의 신설 또는 보완과 관련하여 가능한 접근으로는 사전규제 신설, 사후규제 시스템의 보완 및 강화가 고려될 수 있다.

일반적으로 규제체계란 규제주체가 어떤 특정한 공익적인 목적을 위하여 규범의 수범자인 국민(규제객체)을 상대로 각종 권리를 제한하거나 의무를 부과함으로써 그와 같은 목적을 유기적으로 수행하는 인적, 물적, 제도적인 결합체를 의미한다¹⁰⁵⁾. 따라서 규제체계란 규제를 집행하는 주체로서 규제기관, 규제의 대상, 규제의 근거로서 각종 규제법령, 그리고 실질적으로 규제를 달성하는 행정작용으로서 각종 규제행위 내지 규제를 그 요소로 한다.

사전규제란 어떤 행위를 하기 전에 법령에 의하여 규제기관에 신고 · 등록 등의

104) 2020. 10. 5.자 조선비즈 기사 - '범죄 악용 '딥페이크' 발전속도 빨라... MS·페북 방어전선 한계', https://biz.chosun.com/site/data/html_dir/2020/10/05/2020100502248.html

105) 이하 규제체계 및 사전, 사후규제 개념에 대한 일반론은 정보통신정책연구원(KISDI), 방송통신 진화에 따른 규제체계 고도화방안 연구, 2010. 12. 를 참고한 것임

행위 또는 인 · 허가 등 규제기관의 행위를 필요로 하거나, 어떤 행위를 하기 전에 개별적이고 구체적인 의무를 부과함으로써 위법성 판단이 행위 이전에 개별적 구체적으로 제시되어 별도의 위법성 판단이 필요하지 않는 경우를 의미한다.

사후규제란 행위 이후에 구체적인 의무를 부과하거나 어떤 행위에 대한 위법성 판단이 행위를 한 후에 규제기관의 별도의 판단 작용에 의하여 비로소 구체화되거나 명확해지는 경우를 의미한다.

딥페이크에 관한 사전규제책으로는 영상 생성 후 유통 전 단계에서의 신고, 허가제, 즉, 딥페이크 유통신고·허가제의 신설이 고려될 수 있다. 딥페이크에 관한 사후규제책으로는 워터마크, 변경내용표시 의무화 등이 고려될 수 있다.

한편, 딥페이크 관련 기술에 대한 실효적인 대응을 위하여 딥페이크로 인한 피해자 구제, 딥페이크 식별 기술의 지원을 위한 기관, 부처 등에 관한 논의도 필요하다.

이하에서는 딥페이크 관련 사전규제책과 사후규제책의 내용 및 도입방안, 한계점 등에 관하여 살펴보고, 딥페이크 기술을 전문적으로 다룰 기관 또는 부처에 관하여도 검토하도록 한다.

제2절 딥페이크 관련 사전규제 방안

1. 딥페이크 유통신고·허가제

가. 서설

딥페이크와 관련한 사전규제책으로는 영상 유통 신고·허가제가 있을 수 있다. 딥페이크 기술을 활용한 영상을 제작한 자로 하여금, 영상 제작(생성) 후 유통 이전에 관계 부처 또는 민간자율기구에 해당 영상물을 신고하거나 유통 허가를 받도록 할 의무를 부과하는 제도를 말한다.

한 번 유통되면 피해를 회복하기 어려운 딥페이크 영상의 특성상, 영상 유통 신고·허가제는 가장 강력한 규제이기는 하나, 딥페이크 영상을 언론·출판의 자유 보호대상에 속하는 의사표현 수단이라고 본다면, 사전 신고·허가제는 헌법 제21조 제2항에서 금지하는 사전검열에 해당할 수 있다.

이하에서는 딥페이크에 영상 유통 신고·허가제를 적용할 수 있을지에 관하여 검토한다.

나. 딥페이크 유통신고·허가제의 도입가능성

딥페이크에 대한 유통·허가제에 대하여 사전검열 논란이 있을 수 있다.

우리 헌법은 검열을 금하고 있을 뿐 그에 관한 법적 정의를 내리고 있지 아니하나, 헌법재판소는 1996. 10. 4. 93헌가13등 사건에서 헌법이 금지하는 검열의 개념에 관하여 "행정권이 주체가 되어 사상이나 의견 등이 발표되기 이전에 예방적 조치로서 그 내용을 심사, 선별하여 발표를 사전에 억제하는, 즉 허가받지 아니한 것의 발표를 금지하는 제도"를 뜻하며, "그 명칭이나 형식에 구애됨이 없이 실질적으로 위에서 밝힌 검열의 개념에 해당되는 모든 것을 그 대상으로 하는 것"이라고 정의하고, 그 절차에

관하여 검열은 일반적으로 허가를 받기 위한 표현물의 제출의무, 행정권이 주체가 된 사전심사절차, 허가를 받지 아니한 의사표현의 금지 및 심사절차를 관철할 수 있는 강제수단 등의 요건을 갖추어야 한다고 판시한 바 있다.

헌법재판소는 위 사건(1996. 10. 4. 93헌가13등)에서 영화도 의사표현의 한 수단이므로 헌법 제21조에 의한 언론출판의 자유와 헌법 제22조에 의한 학문과 예술의 자유의 보장을 받는다고 전제하고, 따라서 영화에 대한 허가나 검열은 인정되지 아니한다고 하면서, 영화법 해당 조문이 위헌이라고 결정하였다.

헌법재판소 1996. 10. 4. 93헌가13등 병합결정(이른바, 영화검열 사건)

1. 영화도 의사표현의 한 수단이므로 영화의 제작 및 상영은 다른 의사표현수단과 마찬가지로 언론·출판의 자유에 의한 보장을 받음은 물론, 영화는 학문적 연구결과를 발표하는 수단이 되기도 하고 예술표현의 수단이 되기도 하므로 그 제작 및 상영은 학문·예술의 자유에 의하여도 보장을 받는다.

2. 가. 헌법(憲法) 제21조 제2항의 검열은 **행정권이 주체가 되어 사상이나 의견 등이 발표되기 이전에 예방적 조치로서 그 내용을 심사, 선별하여 발표를 사전에 억제하는, 즉 허가받지 아니한 것의 발표를 금지하는 제도를 뜻한다.** 그러므로 검열은 일반적으로 허가를 받기 위한 표현물의 **제출의무**, 행정권이 주체가 된 **사전심사절차**, **허가를 받지 아니한 의사표현의 금지 및 심사절차를 관철할 수 있는 강제수단** 등의 요건을 갖춘 경우에만 이에 해당하는 것이다.

나. 헌법(憲法) 제21조 제1항이 언론·출판에 대한 검열금지를 규정한 것은 비록 헌법(憲法) 제37조 제2항이 국민의 자유와 권리를 국가안전보장·질서유지 또는 공공복리를 위하여 필요한 경우에 한하여 법률로써 제한할 수 있도록 규정하고 있다고 할지라도 언론·출판에 대하여는 검열을 수단으로 한 제한만은 법률로써도 허용되지 아니한다는 것을 밝힌 것이다.

다. 검열금지의 원칙은 모든 형태의 사전적인 규제를 금지하는 것이 아니고 단지 의사표현의 발표 여부가 오로지 행정권의 허가에 달려있는 사전심사만을 금지하는 것을 뜻하며, 또한 정신작품의 발표 이후에 비로소 취해지는 사후적인 사법적 규제를 금지하지 않는다. 따라서 심의기관에서 허가절차를 통하여 영화의 상영 여부를 종국적으로 결정할 수 있도록 하는 것은 검열에 해당하나, 예컨대 영화의 상영으로 인한 실정법위반의 가능성을 사전에 막고, 청소년 등에 대한 상영이 부적절할 경우 이를 유통단계에서 효과적으로 관리할 수 있도록 미리 등급을 심사하는 것은 사전검열이 아니다.

3. 가. 영화법(映畵法) 제12조 제1항, 제2항 및 제13조 제1항이 규정하고 있는 영화에

대한 심의제의 내용은 심의기관인 공연윤리위원회가 영화의 상영에 앞서 그 내용을 심사하여 심의기준에 적합하지 아니한 영화에 대하여는 상영을 금지할 수 있고, 심의를 받지 아니하고 영화를 상영할 경우에는 형사처벌까지 가능하도록 한 것이 그 핵심이므로 이는 명백히 헌법(憲法) 제21조 제1항이 금지한 사전검열제도를 채택한 것이다.

나. 검열을 행정기관이 아닌 독립적인 위원회에서 행한다고 하더라도 행정권이 주체가 되어 검열절차를 형성하고 검열기관의 구성에 지속적인 영향을 미칠 수 있는 경우라면 실질적으로 검열기관은 행정기관이라고 보아야 한다. 그러므로 공연윤리위원회가 민간인으로 구성된 자율적인 기관이라고 할지라도 영화법(映畵法)에서 영화에 대한 사전허가제도를 채택하고, 공연법에 의하여 공연윤리위원회를 설치토록 하여 행정권이 공연윤리위원회의 구성에 지속적인 영향을 미칠 수 있게 하였으므로 공연윤리위원회는 검열기관으로 볼 수밖에 없다.

이후 건강기능식품광고 사전심의 사건(2018. 6. 28. 2016헌가8), 방송광고 사전심의 사건(2008. 6. 26. 2005헌마506) 등에서 헌법재판소는 사전검열 요건에 관한 위와 같은 법리에 기초하여, 사전 심의 의무를 부과한 근거 범조항에 대하여 위헌을 선언하였다.

헌법재판소 2018. 6. 28. 2016헌가8 등(건강기능식품광고 사전심의 사건)

광고의 심의기관이 행정기관인지 여부는 기관의 형식에 의하기보다는 그 실질에 따라 판단되어야 하고, 행정기관의 자의로 개입할 가능성이 열려 있다면 개입 가능성의 존재 자체로 헌법이 금지하는 사전검열이라고 보아야 한다. 건강기능식품법상 기능성 광고의 심의는 식약처장으로부터 위탁받은 한국건강기능식품협회에서 수행하고 있지만, 법상 심의주체는 행정기관인 식약처장이며, 언제든지 그 위탁을 철회할 수 있고, 심의위원회의 구성에 관하여도 법령을 통해 행정권이 개입하고 지속적으로 영향을 미칠 가능성이 존재하는 이상 그 구성에 자율성이 보장되어 있다고 볼 수 없다. 식약처장이 심의기준 등의 제정과 개정을 통해 심의 내용과 절차에 영향을 줄 수 있고, 식약처장이 재심의를 권하면 심의기관이 이를 따라야 하며, 분기별로 식약처장에게 보고가 이루어진다는 점에서도 그 심의업무의 독립성과 자율성이 있다고 어렵다. 따라서 이 사건 건강기능식품 기능성광고 사전심의는 그 검열이 행정권에 의하여 행하여진다고 볼 수 있고, 헌법이 금지하는 사전검열에 해당하므로 헌법에 위반된다.

헌법재판소 2008. 6. 26. 2005헌마506(방송광고 사전심의 사건)

한국광고자율심의기구는 행정기관적 성격을 가진 방송위원회로부터 위탁을 받아 이 사건 텔레비전 방송광고 사전심의를 담당하고 있는바, 한국광고자율심의기구는 민간

이 주도가 되어 설립된 기구이기는 하나, 그 구성에 행정권이 개입하고 있고, 행정법상 공무수탁사인으로서 그 위탁받은 업무에 관하여 국가의 지휘·감독을 받고 있으며, 방송위원회는 텔레비전 방송광고의 심의 기준이 되는 방송광고 심의규정을 제정, 개정할 권한을 가지고 있고, 자율심의기구의 운영비나 사무실 유지비, 인건비 등을 지급하고 있다. 그렇다면 한국광고자율심의기구가 행하는 방송광고 사전심의는 방송위원회가 위탁이라는 방법에 의해 그 업무의 범위를 확장한 것에 지나지 않는다고 할 것이므로 한국광고자율심의기구가 행하는 이 사건 텔레비전 방송광고 사전심의는 행정기관에 의한 사전검열로서 헌법이 금지하는 사전검열에 해당한다.

헌법재판소에서 정리한 사전검열제도 요건을 정리하면, 우선 기본적 전제로서 사전심사절차를 거치지 않은 정보의 전파를 일반적으로 금지하고, 그 금지에 위반한 경우 이를 처벌하는 체제로 구성되며, 일반적으로 ① 표현·전파될 정보의 수집 ② 심사 ③ 제한조치 및 집행 ④ 제한 위반 시 제재 등의 단계로 구분된다.

나아가 헌법재판소 결정례에서 도출할 수 있는 사전검열의 합헌요건¹⁰⁶⁾은 ① 순수한 자율규제 형태의 규제기구, ② 심의절차가 법익의 충돌을 조정하여 올바른 형량과 결론을 담보하기 위해 헌법상 적법절차에 따라 이루어질 것, ③ 적용대상 심의기준의 명확성, ④ 제재 및 제한의 정도가 헌법상 허용될 수 있는 수준일 것 등이 있다.

딥페이크의 악용가능성을 별론으로 하고, 일단 딥페이크 영상물 자체가 의사 표현의 수단인 이상 이를 표현의 자유 보호 영역에서 제외된다고 보기는 어렵다. 헌법재판소가 제시한 사전검열제도의 요건에 비추어, 딥페이크 영상에 대한 사전 신고·허가제는 사전검열에 해당할 여지가 크다.

먼저 순수한 형태의 자율기구 신설 및 운영은 현실적으로 기대하기 어렵다. 헌법재판소는 앞서 소개한 방송광고 사전심의 사건에서, 민간자율기구 형태로 운영되는 방송통신심의위원회의 법적 성질에 관하여 다음과 같이 판단하였다.

헌법재판소 2008. 6. 26. 2005헌마506(방송광고 사전심의 사건)

(전략)방송광고사전심의의 주체를 방송통신심의위원회로 변경하였는데, 방송통신심의

106) 박용상, 헌법상 사전검열금지의 원칙, 법학논집 제21호, 2010, 211면 이하

위원회의 구성이나 업무, 업무처리 방식 등은 구 방송위원회의 그것과 다르지 않다고 할 것인바, 법질서의 정합성과 소송경제의 측면에서 개정된 방송법에 대해서도 위헌을 선언(후략)

이는 곧 방송법 개정 전 방송위원회와 방송법 개정 후 방송통신심의위원회의 법적 성질이 동일하다고 본 것으로서, 방송위원회의 성격에 대한 헌법재판소의 법적 판단(행정기관적 성격)이 방송통신심의위원회에도 그대로 적용됨을 의미한다. 방송통신심의위원회는 방송과 통신 심의와 관련해, 독립적으로 사무를 수행하는 민간주도의 행정기구임을 표방하나, 구조적 측면과 위원구성에 있어서 비독립적인 합의제 행정기관으로서의 위상을 보여주고 있다¹⁰⁷⁾. 따라서 방송통신심의위원회가 주체가 된 사전심의는 헌법이 금지하는 사전검열에 해당한다고 볼 수 밖에 없다.

심의기준과 관련하여서도 합헌 요건을 준수하기란 어려울 것으로 예상된다. 사후규제를 전제하고 운영 중인 현행 정보통신에 관한 심의규정을 딥페이크 사전 규제에 그대로 적용하기 어려우며, 관련 심의 기준의 입안 주체, 절차 등에 있어서 행정권의 영향을 완전히 배제할 것을 기대하기가 현실적으로 어렵기 때문이다.

이상의 이유로 합헌요건을 준수한 형태의 사전 신고·허가제 운영은 현행법 하에서 대단히 어려울 것으로 예상된다. 따라서 딥페이크 영상을 대상으로 한 사전 신고·허가제 운영은 불법적 딥페이크 영상 유통 규제 목적을 달성하기 위한 현실적인 대안이 되기 어렵다.

다. 소결

이상과 같이 딥페이크 영상물 유통 신고·허가제를 운영하기 위해서는 헌법재판소에서 제시한 까다로운 합헌요건을 준수하여야 하나, 이는 현실적으로 기대하기 어렵다.

2. 결어

107) 심재철, 오미영, 방송통신심의위원회의 위상과 나아갈 방향에 대한 시론, 2011, 6면

딥페이크에 대한 사전규제책으로서의 유통 신고·허가제는 가장 확실하고 강력하게 딥페이크를 규제할 수 있다는 장점이 있으나, 이상에서 본 바와 같이 헌법상 사전 검열에 해당하여 실제로 추진하기 쉽지 않다.

따라서 딥페이크에 대한 사전규제책 보다는 사후규제책에 집중하여 딥페이크 기술로 인한 사회적 부작용을 줄이고 순기능을 더욱 촉진할 수 있는 방향을 찾는 것이 바람직하다.

이하에서는 딥페이크에 관한 사후규제책으로 딥페이크 영상 생성 이후 유통시 워터마크, 서명, 라벨 등 표시의무화, 변경내용표시의무화 등의 제도 도입가능성에 관하여 살펴보고, 딥페이크 영상 유통으로 인한 피해자의 구제강화를 위한 방안에 관하여 검토하도록 한다.

제3절 딥페이크 관련 사후규제 방안

1. 워터마크·전자서명 등을 이용한 딥페이크 표시의무제도

1.1. 서설

딥페이크는 음란물, 가짜뉴스, 명예훼손 등 범죄에 악용될 가능성이 있는바, 딥페이크의 제작은 제작자들의 자율에 맡기되, 다만 유통되는 딥페이크에 딥페이크 기술에 의하여 만들어진 영상이라는 점을 표시하도록 할 수 있다. 딥페이크라는 표시방법으로 현행 기술인 워터마크, 전자서명, 라벨 등의 적용을 검토할 수 있다.

딥페이크에 워터마크, 전자서명, 라벨 등이 가시적으로 표시되면 시청자로 하여금 딥페이크 기술로 인한 가공된 영상이라는 점을 인지시켜 가짜뉴스, 명예훼손 등에 의한 피해를 줄일 수 있을 것이다. 또한 딥페이크에 워터마크 등이 비가시적으로 표시되더라도 해당 영상이 문제될 경우 워터마크 등의 검출 기술을 이용하여 딥페이크라는 점을 곧바로 알아낼 수 있으므로 피해의 확산을 방지할 수 있다.

이하에서는 딥페이크에 대한 워터마크, 전자서명, 라벨 등의 도입가능성 에 관하여 살펴본다.

1.2. 디지털 워터마크

가. 개념

디지털 워터마크(Digital Watermark)는 디지털 콘텐츠에 그 권리자만이 알 수 있는 아이디(ID) 또는 정보 등의 부호를 삽입하거나, 영상·음성 등의 신호에 특정한 코드나 유형 등을 삽입한 것 또는 그 기술을 지칭하는 것으로, 사후에 디지털 정보의 지

적재산권을 보호할 수 있도록 하는 기술이다¹⁰⁸⁾. 디지털 워터마크는 디지털 상태의 동영상, 그림, 텍스트, 음악파일 등에 삽입된 로고나 상표 등의 마크를 뜻한다.

디지털 콘텐츠의 특성상 원본의 손상 없이 무제한의 복제와 유통이 가능하고, 원본과의 구별이 불가능하여 저작권의 보호나 불법 복제·유통의 방지 등이 갈수록 필요해지고 있다. 이에 디지털 워터마크는 디지털 콘텐츠 소유자의 권리를 보호하기 위한 대안 중 하나로 등장하였다.

현재 국내에서 디지털 워터마크는 온라인상의 콘텐츠 위변조 판별, 무단 배포 방지, 사용자 제어, 저작권 주장 등에 활용되고 있다¹⁰⁹⁾.

디지털 워터마크는 보통 연성 워터마킹 기술을 이용하기 때문에 온라인 상에서 편집이나 수정시 워터마킹된 부분이 깨지게 되므로 이를 통해 문서의 진위여부를 판별할 수 있다. 예를 들면 다른 사람이 워터마킹이 된 문서를 사용하여 일부를 수정한 후에 이를 사용하려고 할 때 원 저작권자는 이 파일의 워터마크 상태를 검사하여 이 파일이 원본인지 아니면 변조된 것인지 확인할 수 있다.

또한 워터마킹 기술을 사용해서 이미지 또는 영상이 만들어진 시간, 제작자 등과 같은 정보를 심을 수 있고, 복사된 것이라는 표시를 할 수 있다. 또한 멀티미디어 콘텐츠를 복사하거나 재생하는 데 특별한 하드웨어 장치가 필요한 경우, 디지털 워터마크가 콘텐츠에 삽입되어 콘텐츠를 복사할 수 있는 횟수 등을 제어하는 데 사용될 수 있다.

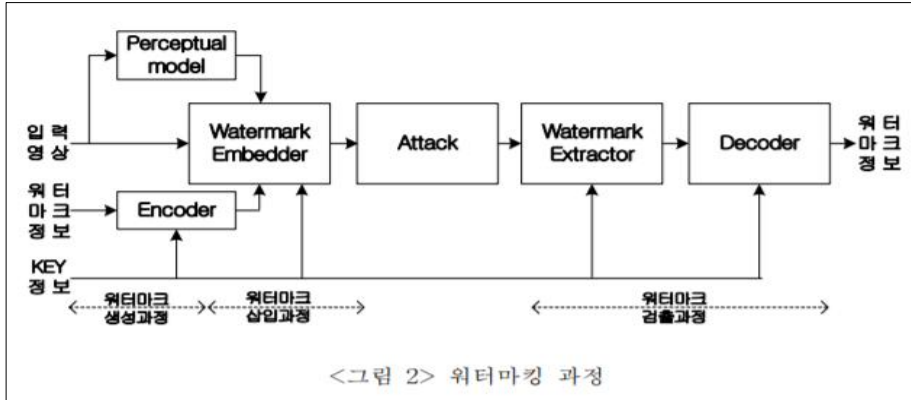
나. 디지털 워터마크의 기술 개요

디지털 워터마킹 기술은 크게 워터마크 생성(generation), 삽입(embedding) 및 검출(detecting) 기술로 구분 된다.

108) 강상익, 디지털 워터마킹 국내·외 표준화 동향, TTA저널 제73호, 2001, p.139 참조.

109) 오병택·문병주·이동일, 디지털 워터마킹 기술동향 및 전망, 전자통신동향분석 제17권 6호, 2002, p.157 참조.

[그림 4-1] 워터마킹 기술의 적용 과정



자료 :

http://www.huchems.com/media/news/news_cyber06_93398393241c909b4c5b0e.pdf.
p3-5.

'워터마크 생성과정'은 삽입하고자 하는 워터마크를 어떤 형태로 대상 콘텐츠에 삽입할 것인지 결정하는 방법이다. 워터마크는 이진(binary) 영상, 키(key) 값에 의해 변환된 이진 영상, 키 정보에 의해 암호화된 문자열 또는 유사잡음(pseudonoise) 신호등이 사용된다. 이러한 워터마크는 워터마크의 유무 정보뿐만 아니라 '저작권', '소유자', '콘텐츠 내용' 등을 포함할 수 있으며, 이렇게 워터마크에 삽입되는 내용을 워터마크 페이로드(payload)라 정의한다.

'워터마크 삽입과정'은 생성된 워터마크를 어떻게 원본 영상에 삽입할 것인지 결정하는 과정이다. 대부분의 디지털 이미지/동영상 워터마킹에서 워터마크의 비가시성(invisibility)을 위하여 인간시각시스템의 특성을 고려한 모델을 적용하여 삽입하게 된다. 그러나 디지털 워터마크는 반드시 비가시성을 목적으로 하는 것이 아니며, 눈에 보이게 하는 워터마크의 삽입도 선택적으로 가능하다.

'워터마크의 검출과정'은 크게 원본 콘텐츠의 사용 여부에 따라서 두 가지로 나뉜다. 원본을 가지고 하는 널블라인드 검출방식으로는 원본 콘텐츠와의 차 값을 이용하

는 방법과 원본과의 유사도를 측정하는 워터마크 검출법이 있다. 블라인드 검출방식으로는 워터마크 신호의 자기상관도(autocorrelation)를 구하는 방식, 정합 필터(matched filter)을 이용한 방식 또는 확률적인 방법을 응용한 MAP(Maximum A-Posteriori)을 이용하는 방식 등이 있다.

워터마크는 워터마크가 없는 부분만을 잘라내거나 워터마크를 제거함으로써 워터마크가 삭제될 수 있다는 기술적인 한계점을 지니고 있다.

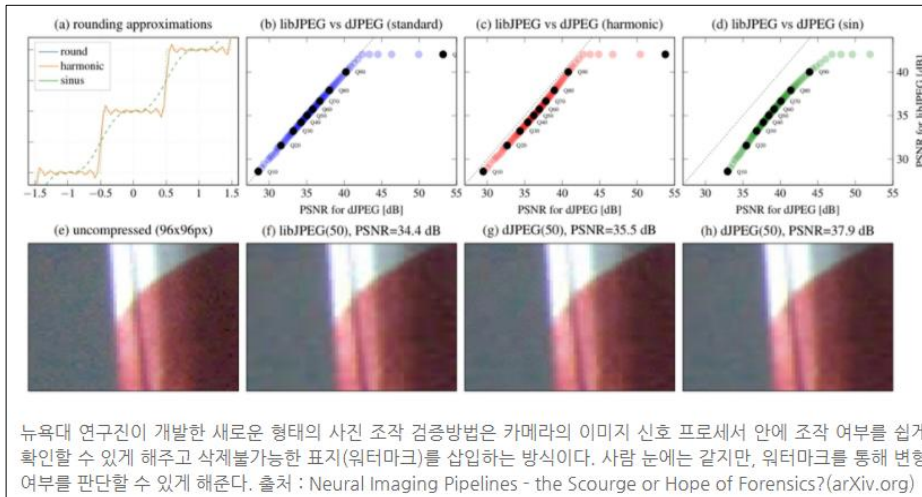
그러나 미국의 정보기술전문지 <WIRED>에 따르면, 최근 뉴욕대학의 텐던공대(New York University's Tandon School of Engineering) 연구팀은 카메라에서 이미지를 생성하는 시점에 포렌식 정보를 내장하는 방식으로 딥페이크 유무를 확인하는 카메라 촬영 기술을 개발하였다고 한다¹¹⁰⁾.

연구팀은 이미지에 복제방지 표지(워터마크)를 삽입하거나 해시값을 검증하는 기존 위조방지 기술의 경우, 워터마크는 복제되거나 삭제될 수 있고, 해시값은 사진이 편집되거나 복제될 때마다 달라지므로 사진이 다양하게 활용되는 상황에서 적용에 한계가 있다는 점을 지적하면서, 금번 발표한 위조방지 기술은 카메라의 이미지 신호 프로세서 안에 조작 여부를 쉽게 확인할 수 있게 해주고 삭제 불가능한 표지(워터마크)를 삽입하는 방식을 통해 조작 여부를 쉽게 확인할 수 있을 뿐만 아니라, 동시에 삭제가 불가능한 워터마크를 생성단계에서 삽입함으로써 기존 위조방지 기술의 한계점을 극복할 수 있다고 하였다¹¹¹⁾.

110) <https://webcache.googleusercontent.com/search?q=cache:kFEFNcB89UgJ:https://www.wired.com/story/detect-deepfakes-camera-watermark/+&cd=1&hl=ko&ct=clnk&gl=kr>

111) <http://www.hani.co.kr/arti/PRINT/897415.html>

[그림 4-2] 뉴욕대 연구진이 개발한 새로운 형태의 사진 조작 검증방법



자료 : <http://www.hani.co.kr/arti/PRINT/897415.html>

이 워터마크는 이미지의 내용이 변형되면 알려주는 기능을 하는데, 연구팀은 이 포렌식 친화적 촬영 기능을 사용한 결과, 조작사진 탐지율이 기존 45%에서 90% 이상으로 높아졌다고 밝혔다. 하지만 연구팀은 카메라의 이미지 프로세서에 워터마크 기술을 채택하는 포렌식 친화적 위조방지 기술 또한 완벽할 수는 없다고 한계를 인정하면서, 가짜와 위조를 탐지하는 다른 접근법과 함께 사용될 때 효과를 높일 수 있다는 제안을 하였다.

이러한 기술을 활용하여 딥페이크 생성단계에서 삭제 불가능한 워터마크를 삽입하는 방안이 고려될 수 있다.

다. 디지털 워터마크 관련 국내외 제도 및 입법현황

1) 국내의 경우

국내 행정규칙 중 통합문서관리시스템운영지침은 제3조 제8호에서 워터마크에 관하여, "시스템내의 문서에 대하여 출력 시 공단 문서임을 증명하고 무단유출을 방지하기 위하여 공단 CI, 사용자 정보, 출력일시를 출력물에 전자적으로 삽입 출력하는 것"이라고 정의함으로써, 워터마크를 문서의 증명 및 무단배포 방지수단으로 활용하고 있다.

통합문서관리시스템운영지침 [근로복지공단지침 제2007-4호]

제3조 (정의) 이 지침에서 사용하는 용어의 정의는 다음과 같다.

8. "워터마크(WaterMark)"라 함은 시스템내의 문서에 대하여 출력 시 공단 문서임을 증명하고 무단유출을 방지하기 위하여 공단 CI, 사용자 정보, 출력일시를 출력물에 전자적으로 삽입 출력하는 것을 말한다.

또한 병무행정 정보업무 관리규정(병무청훈령인)은 제33조 제1항에서는 "병역자료 등 개인정보 및 중요자료의 유출·노출을 차단하기 위하여 병무청의 모든 정보화 기기의 기술적·관리적 안전성을 확보하기 위한 조치를 취해야 한다"고 규정하면서, 동 조 제2항에서 "개인용 컴퓨터 등 정보화 기기를 통한 출력물에는 워터마킹 처리를 하여야 한다"고 규정하고 있고, 방위산업기술 보호지침(방위사업청훈령) 제30조 제4항에서는 "대상기관의 장은 관리대상기술 취급을 허가받지 않은 자가 관리대상기술의 전산자료에 접근할 때에는 이를 경고하여야 하며, 출력할 때에는 출력 일시, 워터마크 및 출력한 컴퓨터의 고유번호가 자동으로 표시되도록 하고, 출력물 불법유출에 대한 보호대책을 강구한다"고 규정하여, 워터마크를 자료의 무단배포 방지수단으로 활용하고 있다.

병무행정 정보업무 관리규정 [병무청훈령 제1470호]

제33조(자료보호)

① 병역자료 등 개인정보 및 중요자료의 유출·노출을 차단하기 위하여 병무청의 모든 정보화 기기의 기술적·관리적 안전성을 확보하기 위한 조치를 취해야 한다.

② 개인용 컴퓨터 등 정보화 기기를 통한 출력물에는 워터마킹 처리를 하여야 한다. 다만, 각종 증명서와 통지서 및 외부에 제공되는 문서의 출력물에는 워터마킹 적용을 해제할 수 있으며 이를 위한 개인용 컴퓨터는 최소한으로 제한하여야 한다.

방위산업기술 보호지침 [방위사업청훈령 제620호]

제30조(전산자료 보호대책 및 접근범위 제한)

④ 대상기관의 장은 관리대상기술 취급을 허가받지 않은 자가 관리대상기술의 전산자료에 접근할 때에는 이를 경고하여야 하며, 출력할 때에는 출력 일시, 워터마크 및 출력한 컴퓨터의 고유번호가 자동으로 표시되도록 하고, 출력물 불법유출에 대한 보호대책을 강구한다.

한편, 국내에는 아직 딥페이크 영상에 대하여 워터마크의 삽입을 의무화하는 법령이나 법안이 마련되어 있지는 않다.

2) 해외의 경우

EU는 2018년 딥페이크를 비롯한 허위정보 전반에 대응하기 위한 전략(Communication-Tackling online disinformation: a European Approach)을 발표하고, 모든 형태의 허위정보식별을 위해 정보의 출처 및 신뢰성 여부를 쉽게 알 수 있도록 조치하도록 하였으나¹¹²⁾, 아직 구체적으로 어떠한 조치가 이루어지고 있는지 확인되지는 아니하며, 위 전략의 내용상 관련 조치가 반드시 워터마크일 것임을 전제하지 않고 있다.

중국은 2019. 12. 딥페이크와 같은 영상 조작에 관한 규제 조항을 포함한 법률 '네트워크 오디오 및 비디오 정보 서비스 관리규정(网络音视频信息服务管理规定, Regulations on the Administration of Network Audio and Video Information Services)'을 제정하여 온라인 오디오·영상정보서비스 제공자 및 온라인 오디오·영상정보서비스 사용자는 리얼 러닝 및 가상 현실¹¹³⁾이라는 점을 표시하여야 한다는 점을 명시하

112) 김유향, 딥페이크(Deepfake)의 발전과 해외 법제도 대응, p.4 참조.

113) 위 개념에는 딥페이크 영상이 포함된다.

고 있으나(제11조), 그 표시가 반드시 워터마크일 것에 관하여는 명시하지 않고 있다.

딥페이크 영상에 워터마크라는 기술을 이용할 것을 명시적으로 요구하고 있는 것은, 미국의 2019년 책임법에 따라 부당한 이용으로부터 유래한 허위의 외관으로부터 모든 사람들을 보호하기 위한 법률(Defending Each and Every Person from False Appearances by Keeping Exploitation Subject to Accountability Act of 2019)이다.

위 법안은 2019. 6. 13. 에너지통상위원회(Committee on Energy and Commerce), 2019. 6. 24. 국토안보위원회(Committee on Homeland Security), 2019. 6. 28. 법사위원회(Committee on the Judiciary)에 각 회부되어 있는 상황으로 아직 정식으로 시행되고 있는 법률은 아니다.

다만 딥페이크에 관하여 구체적으로 다루면서 그 규제책의 하나로서 워터마크 기술을 상세히 언급하고 있어 주목할 필요가 있다.

위 법안은 딥페이크를 '(A) 실제로 그러한 언행에 관여하지 않은 사람의 말이나 행동을 사실적으로 묘사하는 것으로 보이는 것 또는 (B) 다른 사람의 신체적 언어적 능력보다는 기술적 수단에 실질적으로 의존한 것에 관한 영상 녹화, 영화용 필름, 음성 녹음, 전자 이미지 또는 사진, 언어의 기술적 표현 또는 실질적으로 파생된 행위라고 정의하면서(SEC. 2 (n)(3)), 주간(interstate) 또는 외국과의 상거래 수단이나 시설을 이용하여, 인터넷을 통해 배포하려는 의도로 첨단 기술 허위 개인화 기록(an advanced technological false personation record)을 생산하거나 그 기록이 배포되어야 하는 지식을 생산하는 자는, (b)항에 따른 '워터마크' 요구 사항¹¹⁴⁾, 시청각기록의 경우 (c)항에 따른 공개요건, 영상기록의 경우 (d)항에 따른 공개요건, 오디오 레코드의 경우 (e)항에 따른 공개 요건을 준수하여야 한다고 정하고 있다(SEC. 2 (a)).

위 법안이 적용되는 경우 움직이는 시각적 요소를 포함하는 첨단 기술 허위 개인화 기록(an advanced technological false personation record)에는 변경된 오디오 또는 시각적 요소를 식별할 수 있도록 내장형 '디지털 워터마크'를 포함하여야 한다.(SEC. 2

114) (b)항의 워터마크 요건은 법무부장관(the Attorney General)이 규정으로 결정한 첨단 기술 허위인격기록의 등급에 대해서는 적용되지 않는다(SEC. 2 (j)(2)).

(b)),

위 법안은 누구든지 첨단 기술 허위 개인화 기록(an advanced technological false personation record)을 배포하려는 의도로 (a)항에 따라 요구되는 '워터마크'를 '제거'하거나 공개 요건을 '모호'하게 만드는 경우 벌금 또는 5년 이하의 징역에 처하도록 하였으며(SEC. 2 (f)(1)(B)), 최대 15만 달러의 민사상 벌금과 적절한 금지명령을 받아야 한다고 정하고 있다(SEC. 2 (f)(2)).

또한 위 법안은 본 법안의 제정일로부터 1년 이내에 '디지털 워터마크'의 기술 사양에 관한 규칙을 발표할 의무도 규정하고 있다(SEC. 2 (k),(3)).

3) 소결

위와 같이 국내에는 아직 딥페이크에 워터마크를 삽입할 의무에 관한 법령이나 법안이 없다. 해외에서도 딥페이크에 워터마크를 삽입할 것을 요구하는 법이 시행되고 있지는 아니하며, 미국에서 법안의 형태로만 존재하고 있다.

라. 적용 및 한계점

위에서 살펴본 바와 같이 디지털 워터마크는 이미지 또는 영상 생성 시에 표시될 수 있으며, 현재 대부분의 워터마크는 저작권보호, 불법유통 방지 등을 위하여 제작자가 자율적으로 표시하고 있다. 디지털 워터마크가 삽입된 영상을 원본으로 하여 딥페이크 영상으로 가공할 경우, 워터마크가 훼손되거나 깨지게 되므로 손쉽게 딥페이크 기술이 활용된 가공영상이라는 점을 알아낼 수 있다.

딥페이크 기술로 인한 부작용을 방지하기 위하여, 딥페이크 기술로 만들어진 영상에 워터마크를 표시할 의무를 부과하는 방안을 생각해볼 수 있으며, 딥페이크 영상에 워터마크를 가시적으로 삽입하는 의무를 부과하는 경우 시청자로 하여금 딥페이크 기술로 인한 가공된 영상이라는 점을 인지시켜 가짜뉴스, 명예훼손 등에 의한 피해를

줄일 수 있을 것이다.

나아가 딥페이크 영상에 워터마크를 비가시적으로 삽입하도록 의무화하는 경우, 워터마크 등의 검출 기술을 이용하여 딥페이크 영상이라는 점을 곧바로 알아낼 수 있으므로 더욱 빠르게 피해의 확산을 방지할 수 있다.

그러나 워터마크는 현행 기술상 삭제하는 것이 어렵지 않기 때문에 딥페이크 영상을 완벽하게 식별하기 위한 도구로서는 한계가 있으며, 음성파일 형태로 존재하는 딥페이크의 경우에는 활용하기 어렵다는 문제가 있다.

1.3. 전자서명

가. 개념

'전자서명'은 서명자를 확인하고 서명자가 당해 전자문서에 서명했다는 사실을 나타내는데 이용하기 위하여, 특정 전자문서에 첨부되거나 논리적으로 결합된 전자적 형태의 정보를 의미한다.

전자서명법 제2조 제2호는 '전자서명'에 관하여, "서명자를 확인하고 서명자가 해당 전자문서에 서명을 하였음을 나타내는데 이용하기 위하여 해당 전자문서에 첨부되거나 논리적으로 결합된 전자적 형태의 정보"라고 정의한다.

전자서명법

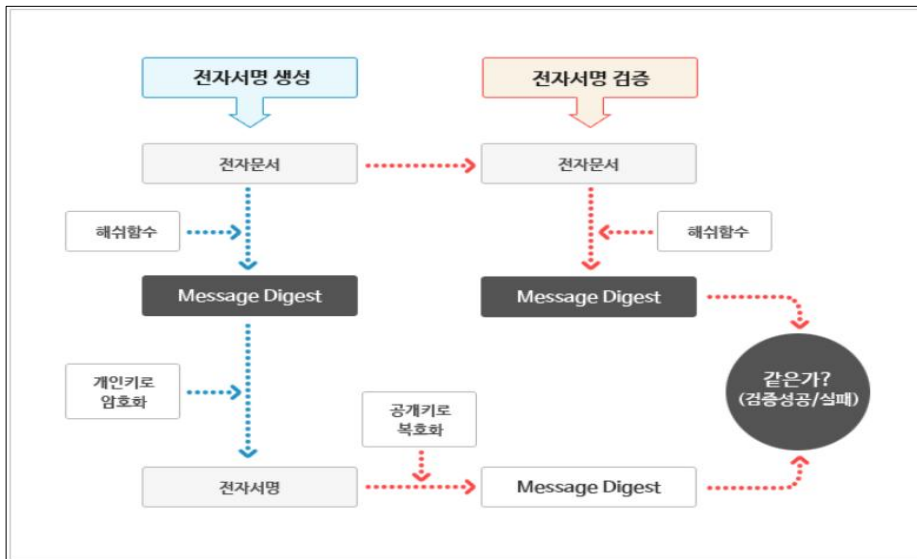
제2조(정의) 이 법에서 사용하는 용어의 정의는 다음과 같다.

2. "전자서명"이라 함은 서명자를 확인하고 서명자가 해당 전자문서에 서명을 하였음을 나타내는데 이용하기 위하여 해당 전자문서에 첨부되거나 논리적으로 결합된 전자적 형태의 정보를 말한다.

즉 전자서명은 종이문서의 서명과 같이 전자문서에 서명한 사람이 누구인지 확인하고 서명된 전자문서의 위·변조사실을 알 수 있도록 전자문서에 부착하는 특수한 형태의 디지털 정보를 말하고, 인감도장의 역할을 하는 '생상'과 인감증명의 역할을 하는 '

검증' 등 한 쌍의 전자서명키로 구성되는데 생성키는 서명자만 보관해서 사용하고 전자서명검증키는 정보통신망을 통해 누구나 알 수 있도록 공개된다.

[그림 4-3] 전자서명의 생성과 검증 과정



자료 : <https://www.yesign.or.kr/home/subIndex/395.do>

나. 전자서명 관련 국내외 제도 및 입법현황

1) 국내의 경우

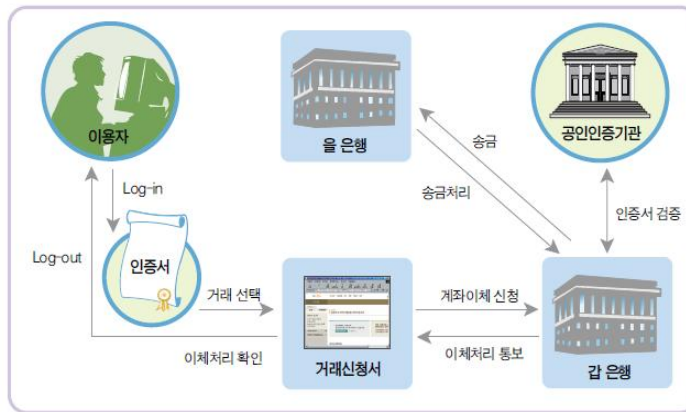
전자서명법은 1999. 2. 5. 전자문서의 안전성과 신뢰성을 확보하고 그 이용을 활성화하기 위하여 전자서명에 관한 기본적인 사항을 정함으로써 국가사회의 정보화를 촉진하고 국민생활의 편익을 증진함을 목적으로 제정되어 현재까지 시행되고 있으며, 전자서명은 인터넷뱅킹, 온라인 증권거래, 전자정부 행정 민원서비스 등에서 주로 상대방 확인 기능, 거래내용의 변경확인 기능, 거래사실의 증명 기능 등으로 활용되고

있다¹¹⁵⁾.

[그림 4-4] 전자서명의 활용

인터넷뱅킹

은행을 직접 방문하지 않고도 인터넷을 통하여 계좌이체, 송금, 대출 등과 같은 은행업무를 안전하게 처리할 수 있습니다.

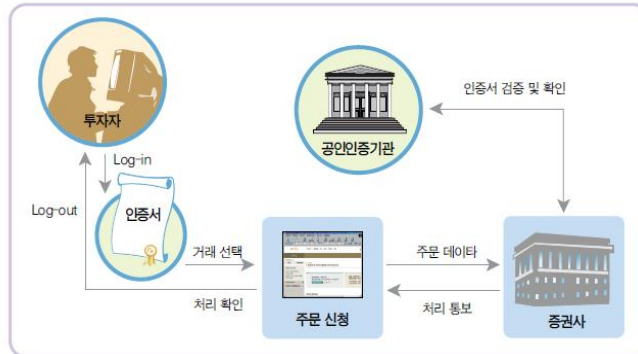


<그림삽입을 위한 여백>

115) 정보통신부·한국정보보호진흥원, 알기쉬운 전자서명, p.12-16 참조.

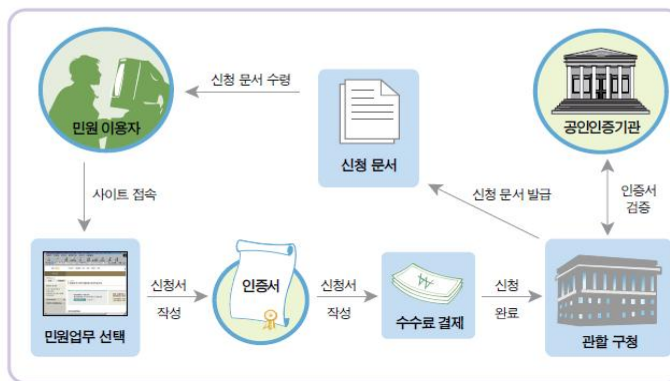
온라인 증권거래

증권사 객장을 방문하거나 전화 이용 없이도 투자자의 신원확인
과 거래 사실이 증명되어 보다 안전한 온라인 증권거래를 수행할 수
있습니다.



전자정부 행정 민원서비스

주민등록등본, 호적등본 발급 등 각종 행정민원업무를 해당기관
을 방문하지 않고도 쉽게 처리할 수 있습니다.



자료 : 정보통신부·한국정보보호진흥원, 알기쉬운 전자서명, p.12-16 참조.

2) 해외의 경우

미국, 독일, 영국, 일본 등의 나라에서도 우리나라 전자서명법과 같이 전자서명인증
제도와 관련하여 법령을 두고 있는데, 각 나라의 전자서명인증제도 관련 입법례를 비

교하면 아래 표와 같다¹¹⁶⁾.

<표 4-1> 전자서명 관련 각국의 입법례

입법례	인증기관에 대한 규제	법적효력 및 업무범위	비 고
한국 전자서명법	요건을 구비한 인증기관을 공인인증기관으로 지정 (공인인증기관지정제도)	공인인증기관이 인증한 전자서명에 전자서명법상의 효력 부여	
미국 연방법	규정 없음 ※ 초기 주법에서 허가제도를 규정하였으나 후발 주들은 등록제 등 완화된 제도 채택	모든 전자서명에 대해 법적 효력 인정 ※ 주법에서 제한	구체적인 사례에 따라 상이한 법적 효력 부여
독일 디지털서명에 관한법률	법에서 정한 요건을 구비한 인증기관이 주무관청에 신고, 주무관청의 확인후 확인필증 수여(임의적 공인인증기관 인정제도)	규정 없음 ※ 개정민법에서 공인전자서명의 서명으로서의 효력을 인정(독일민법 제126조A)	법으로 정하지 않은 전자서명인 경우에는 그 이용이 임의적임
영국 전자통신법	인증기관에 관한 규정 없음 (자율적 비영리기구인 tScheme 에 의한 자발적인 승인시스템으로 운영)	전자서명, 전자서명의 발생, 통신방법, 서명에 사용된 프로시저 등을 증명하는 선언을 한 경우, 개인의 경우에도 전자서명이 인증됨	
일본 전자서명및인 정업무에관한 법률	요건을 구비한 자를 특정인증업무를 수행할 수 있도록 인정(특정인증업무자격 인정제도)	본인에 의한 전자서명이 있을 때에는 전자적 기록이 진정하게 성립된 것으로 추정함	

116) http://privacy.or.kr/wp-content/uploads/2003/04/PT_20021128_LJH.hwp p.8 참조

위와 같이 각 나라별로 전자서명인증제도의 구체적인 내용은 상이하지만, 전자문서를 상대방에게 전송할 때에 당사자를 확인하고, 전자문서에 담긴 내용이 임의로 변경되지 않았다는 것을 밝히는데 전자서명이 이용된다는 점에서는 공통적이다. 즉 전자서명은 당사자의 확인 및 문서내용의 진위 여부를 판단하는 것에 활용된다.

다. 적용 및 한계점

딥페이크 제작자에게 해당 영상에 전자서명을 표시하는 것을 의무로 하여, 해당 영상이 딥페이크 기술로 제작된 영상이라는 점, 딥페이크 제작자가 누구인지 등을 확인할 수 있도록 하는 방안을 생각해볼 수 있다. 전자서명은 서명한 사람에 대한 정보까지 표시되므로, 영상제작자에 대한 책임감을 더욱 높일 수 있다.

그러나 전자서명의 경우 기본적으로 문서를 전제로 한 기술이라는 점에서, 이를 영상에까지 확대하여 적용할 수 있는지에 대한 기술적인 문제가 남아있으며, 음성파일 형태로 존재하는 딥페이크의 경우에는 활용하기 어렵다는 문제가 있다.

1.4. 라벨

가. 개념

'라벨(label)'은 그 복제물이 정당한 권한에 따라 제작된 것임을 나타내기 위하여 저작물 등의 유형적 복제물·포장 또는 문서에 부착·동봉 또는 첨부되거나 그러한 목적으로 고안된 표지를 말한다(저작권법 제2조 제35호).

나. 라벨 관련 제도 및 입법현황

저작권법은 '라벨'에 관하여, "그 복제물이 정당한 권한에 따라 제작된 것임을 나타내기 위하여 저작물등의 유형적 복제물·포장 또는 문서에 부착·동봉 또는 첨부되거나

나 그러한 목적으로 고안된 표지"라고 정의하고(저작권법 제2조 제35호), 누구든지 정당한 권한 없이 ① 라벨 저작물등의 라벨을 불법복제물이나 그 문서 또는 포장에 부착·동봉 또는 첨부하기 위하여 위조하거나 그러한 사실을 알면서 배포 또는 배포할 목적으로 소지하는 행위, ② 저작물등의 권리자나 권리자의 동의를 받은 자로부터 허락을 받아 제작한 라벨을 그 허락 범위를 넘어 배포하거나 그러한 사실을 알면서 다시 배포 또는 다시 배포할 목적으로 소지하는 행위, ③ 저작물등의 적법한 복제물과 함께 배포되는 문서 또는 포장을 불법복제물에 사용하기 위하여 위조하거나 그러한 사실을 알면서 위조된 문서 또는 포장을 배포하거나 배포할 목적으로 소지하는 행위를 하여서는 안 된다고 금지하고 있다(저작권법 제104조의5).

나아가 저작권법은 이를 위반한 자에 대하여는 3년 이하의 징역 또는 3천만원 이하의 벌금에 처하거나 이를 병과할 수 있다고 규정하고 있다(저작권법 제136조 제2항 제3의6호).

이처럼 국내 저작권법은 개별 이용자들로 하여금 정품을 용이하게 판별할 수 있도록 하고, 불법복제 단속의 실효성을 증대함으로써 저작권 보호를 강화하기 위한 방법으로 복제물 등에 라벨을 부착하는 제도를 두고 있다.

다. 적용 및 한계점

이러한 라벨은 기본적으로 원본이 아닌 복제물일 경우를 가정한 제도이다. 딥페이크 영상은 원본 영상이 별도로 있고, 그 영상을 활용하여 또다른 영상을 만드는 것으로 복제물의 속성을 지니고 있다. 이에 딥페이크 제작자에게 딥페이크에 라벨을 부착하는 것을 의무로 하여, 해당 영상이 딥페이크 기술로 제작된 영상이라는 점, 딥페이크의 출처를 확인할 수 있도록 하는 방안을 생각해볼 수 있다.

그러나 라벨은 저작물등의 유형적 복제물·포장 또는 문서에 부착·동봉 또는 첨부되거나 그러한 목적으로 고안된 표지로서, 온라인환경, 디지털환경이 아닌 물리적인 실체가 있는 복제물 등에 사용되는 것을 가정하고 있다.

딥페이크의 경우 이를 저장한 매체가 물리적인 실체를 가지는 경우가 있을 수 있고 그러한 상황에는 라벨이 활용될 여지가 있으나, 주로 온라인 상에서 유통되는 딥페이크의 특성상 라벨부착의 의무화는 딥페이크를 포괄적이고 실효성 있게 규제하는 적절한 수단이 되기 어려운 것으로 보인다.

1.5. 워터마크 표시의무제도의 도입

가. 워터마크 표시의무제도의 적용 범위의 문제

위에서 살펴본 바와 같이 영상의 제작자, 속성 등을 표시할 수 있는 식별혼적심기 방법으로는 디지털 워터마크, 전자서명, 라벨 등이 있다. 다만 전자서명, 라벨 등의 경우에는 디지털 영상에 적용하기 어려운 문제점이 있어, 결국 딥페이크에 대한 식별혼적심기 방안으로는 '디지털 워터마크'가 적절한 것으로 보인다.

딥페이크에 워터마크 표시의무를 부과하는 경우 딥페이크에 대한 워터마크 표시의무를 딥페이크 기술로 생성되는 모든 영상에 대하여 적용할지, 아니면 특정한 딥페이크에 한정하여 적용할지에 대한 문제가 있다.

특정 딥페이크 영상에 대하여 한정하여 워터마크를 표시할 의무를 부과하는 경우, 규제의 대상이 되는 딥페이크의 내용에 관하여 구체적이고 세부적인 기준이 마련되어야 할 것이나 현실적으로 쉽지 않다. 규제의 대상이 되는 딥페이크의 내용으로는 음란물, 명예훼손, 거짓정보 등이 있을 수 있는데 이는 법적인 판단의 영역으로서, 전문성이 있는 기관이 아닌 제작자 스스로가 규제사항에 해당한다는 것을 판단하기가 쉽지 않을 것이기 때문이다.

참고로 정보통신망법 제42조에서는 청소년유해매체물을 제공하려는 자는 대통령령으로 정하는 표시방법에 따라 그 정보가 청소년유해매체물임을 표시하여야 한다고 규정하고, 제42조의2에서 청소년유해매체물의 광고금지에 관하여, 제42조의3에서 청소년보호책임자의 지정에 관하여 규정하고 있다. 나아가 청소년 보호법에서는 청소년유해

매체물의 정의에 관하여 규정하고 관련 고시에서 해당 내용을 상세하게 다루고 있다
(청소년 보호법 제2조 제2호 마목, 제2조 제3호).

정보통신망 이용촉진 및 정보보호 등에 관한 법률

제42조(청소년유해매체물의 표시)

전기통신사업자의 전기통신역무를 이용하여 일반에게 공개를 목적으로 정보를 제공하는 자(이하 “정보제공자”라 한다) 중 「청소년 보호법」 제2조제2호마목에 따른 매체물로서 같은 법 제2조제3호에 따른 청소년유해매체물을 제공하려는 자는 대통령령으로 정하는 표시방법에 따라 그 정보가 청소년유해매체물임을 표시하여야 한다.

제42조의2(청소년유해매체물의 광고금지)

누구든지 「청소년 보호법」 제2조제2호마목에 따른 매체물로서 같은 법 제2조제3호에 따른 청소년유해매체물을 광고하는 내용의 정보를 정보통신망을 이용하여 부호·문자·음성·음향·화상 또는 영상 등의 형태로 같은 법 제2조제1호에 따른 청소년에게 전송하거나 청소년 접근을 제한하는 조치 없이 공개적으로 전시하여서는 아니 된다.

제42조의3(청소년 보호 책임자의 지정 등)

- ① 정보통신서비스 제공자 중 일일 평균 이용자 수, 매출액 등이 대통령령으로 정하는 기준에 해당하는 자는 정보통신망의 청소년유해정보로부터 청소년을 보호하기 위하여 청소년 보호 책임자를 지정하여야 한다.
- ② 청소년 보호 책임자는 해당 사업자의 임원 또는 청소년 보호와 관련된 업무를 담당하는 부서의 장에 해당하는 지위에 있는 자 중에서 지정한다.
- ③ 청소년 보호 책임자는 정보통신망의 청소년유해정보를 차단·관리하고, 청소년유해정보로부터의 청소년 보호계획을 수립하는 등 청소년 보호업무를 하여야 한다.
- ④ 제1항에 따른 청소년 보호 책임자의 지정에 필요한 사항은 대통령령으로 정한다.

청소년보호법

제2조(정의) 이 법에서 사용하는 용어의 뜻은 다음과 같다

2. "매체물"이란 다음 각 목의 어느 하나에 해당하는 것을 말한다.

마. 「전기통신사업법」에 따른 전기통신을 통한 부호·문언·음향 또는 영상정보

3. "청소년유해매체물"이란 다음 각 목의 어느 하나에 해당하는 것을 말한다.

가. 제7조제1항 본문 및 제11조에 따라 청소년보호위원회가 청소년에게 유해한 것으로 결정하거나 확인하여 여성가족부장관이 고시한 매체물

나. 제7조제1항 단서 및 제11조에 따라 각 심의기관이 청소년에게 유해한 것으로 심의하거나 확인하여 여성가족부장관이 고시한 매체물

딥페이크 기술로 만들어진 영상 전체가 아닌 그 중 특정 딥페이크 영상에 대하여 워터마크 표시의무를 부여하는 경우, 위 청소년유해매체물의 경우와 같이 구체적인 내용을 세부적으로 규정하여 제작자가 워터마크를 표시하여야 할지를 판단하기 쉽도록 하여야 한다.

나. 관계 법령 상 워터마크 표시의무제도 도입검토

딥페이크에 대한 워터마크 표시의무제도를 도입할 경우 어떠한 법령에 워터마크 표시의무 관련 규정을 반영하여야 할지 검토하여야 한다.

1) 성폭력처벌법 상 허위영상물 등에 대한 워터마크 표시의무

딥페이크가 가장 문제되고 있는 음란물과 관련된 성폭력처벌법에 관하여 보건대, 성폭력처벌법에서는 애초부터 딥페이크 기술을 이용하여 음란물의 편집, 합성, 가공, 반포등을 금지하고 있는바(성폭력처벌법 제14조의2), 딥페이크 기술로 만든 음란물에 워터마크 표시의무를 부과하는 것은 적절하지 않다.

성폭력범죄의 처벌 등에 관한 특례법

제14조의2(허위영상물 등의 반포등)

① 반포등을 할 목적으로 사람의 얼굴·신체 또는 음성을 대상으로 한 촬영물·영상물 또는 음성물(이하 이 조에서 "영상물등"이라 한다)을 영상물등의 대상자의 의사에 반하여 성적 욕망 또는 수치심을 유발할 수 있는 형태로 편집·합성 또는 가공(이하 이 조에서 "편집등"이라 한다)한 자는 5년 이하의 징역 또는 5천만원 이하의 벌금에 처한다.

② 제1항에 따른 편집물·합성물·가공물(이하 이 항에서 "편집물등"이라 한다) 또는 복제물(복제물의 복제물을 포함한다. 이하 이 항에서 같다)을 반포등을 한 자 또는 제1항의 편집등을 할 당시에는 영상물등의 대상자의 의사에 반하지 아니한 경우에도 사후에 그 편집물등 또는 복제물을 영상물등의 대상자의 의사에 반하여 반포등을 한 자는 5년 이하의 징역 또는 5천만원 이하의 벌금에 처한다.

2) 정보통신망법 상 불법정보에 대한 워터마크 표시의무

정보통신망법 상 딥페이크에 워터마크 표시의무를 반영할 수 있는지 여부에 관하여 보건대, 딥페이크 표시의무제를 시행하고 표시의무위반자에 대한 형사처벌 등 제재조항을 추가할 경우, 표시의무를 이행하지 않은 딥페이크를 정보통신망법 제44조의7 제1항 각 호 중 불법정보의 한 유형으로 보아 이를 제재할 수 있을 것으로 보인다.

정보통신망법 제70조부터 제74조까지가 벌칙규정이며, 그 중 제70조에서 제44조의7 제1항 제1호와 제3호에 대한 처벌규정을 두고 있다. 제70조의 형량은 1년 이하의 징역 또는 1천만원 이하의 벌금으로 정보통신망법의 제70조 내지 제74조의 벌칙규정 중 가장 낮은 수준이다¹¹⁷⁾. 정보통신망법의 현 규정체계상 딥페이크에 대한 워터마크 표시의무는 제44조의7 불법정보의 유통금지 부분에 들어가는 것이 가장 적절하므로, 표시의무위반자에 대한 형량 또한 제44조의7 제1항 각 호 위반자와 동등한 수준으로 규정하는 것이 바람직할 것으로 보인다. 다만 추후 정식으로 제재조항 도입이 결정된다면 1년 이하의 징역 또는 1천만원 이하의 벌금으로 할지, 그보다 더 높거나 더 낮은 수준의 형량으로 정할지, 과태료부와 등 행정벌 수준의 제재에서 그칠지 여부 등 구체적인 형량의 범위가 논의되어야 할 것이다¹¹⁸⁾.

117) 정보통신망법 상 제70조는 3년 이하의 징역 또는 3천만원 이하의 벌금, 7년 이하의 징역, 10년 이하의 자격정지 또는 5천만원 이하의 벌금, 제71조는 5년 이하의 징역 또는 5천만원 이하의 벌금, 제72조는 3년 이하의 징역 또는 3천만원 이하의 벌금, 제73조는 2년 이하의 징역 또는 2천만원 이하의 벌금, 제74조 1년 이하의 징역 또는 1천만원 이하의 벌금을 형량으로 정하고 있다.

118) 아직 통과되어 시행되고 있지는 않지만, 미국의 2019년 책임법에 따라 부당한 이용으로부터 유래한 허위의 외관으로부터 모든 사람들을 보호하기 위한 법률(Defending Each and Every Person from False Appearances by Keeping Exploitation Subject to Accountability Act of 2019)에서는, 누구든지 첨단 기술 허위 개인화 기록(an advanced technological false personation record)을 배포하려는 의도로 (a)항에 따라 요구되는 '워터마크'를 '제거'하거나 공개 요건을 '모호'하게 만드는 경우 벌금 또는 5년 이하의 징역에 처하도록 하였으며(SEC. 2 (f)(1)(B)), 최대 15만 달러의 민사상 벌금과 적절한 금지명령을 받아야 한다고 정하고 있다(SEC. 2 (f)(2)).

다음은 딥페이크 표시의무에 관하여 정보통신망법 제44조의7 제1항 각 호 및 제70조에 법문언을 추가하는 경우의 예시이다. 제44조의7 제1항 아래의 추가되는 문구는 개정된 정보통신망법 제4조 제1항, 제2항 제7의2호¹¹⁹⁾ 인공지능 기술 관련 시책에 사용된 법문언을 참조하였다.

정보통신망 이용촉진 및 정보보호 등에 관한 법률

제44조의7(불법정보의 유통금지 등)

① 누구든지 정보통신망을 통하여 다음 각 호의 어느 하나에 해당하는 정보를 유통하여서는 아니 된다.

1. 음란한 부호·문언·음향·화상 또는 영상을 배포·판매·임대하거나 공공연하게 전시하는 내용의 정보
2. 사람을 비방할 목적으로 공공연하게 사실이나 거짓의 사실을 드러내어 타인의 명예를 훼손하는 내용의 정보
3. 공포심이나 불안감을 유발하는 부호·문언·음향·화상 또는 영상을 반복적으로 상대방에게 도달하도록 하는 내용의 정보
4. 정당한 사유 없이 정보통신시스템, 데이터 또는 프로그램 등을 훼손·멸실·변경·위조하거나 그 운용을 방해하는 내용의 정보
5. 「청소년 보호법」에 따른 청소년유해매체물로서 상대방의 연령 확인, 표시의무 등 법령에 따른 의무를 이행하지 아니하고 영리를 목적으로 제공하는 내용의 정보
6. 법령에 따라 금지되는 사행행위에 해당하는 내용의 정보
- 6의2. 이 법 또는 개인정보 보호에 관한 법령을 위반하여 개인정보를 거래하는 내용의 정보
- 6의3. 총포·화약류(생명·신체에 위해를 끼칠 수 있는 폭발력을 가진 물건을 포함한다)를 제조할 수 있는 방법이나 설계도 등의 정보
7. 법령에 따라 분류된 비밀 등 국가기밀을 누설하는 내용의 정보

119) 정보통신망 이용촉진 및 정보보호 등에 관한 법률

제4조(정보통신망 이용촉진 및 정보보호 등에 관한 시책의 마련)

- ① 과학기술정보통신부장관 또는 방송통신위원회는 정보통신망의 이용촉진 및 안정적인 관리·운영과 이용자 보호 등(이하 "정보통신망 이용촉진 및 정보보호등"이라 한다)을 통하여 정보사회의 기반을 조성하기 위한 시책을 마련하여야 한다.
- ② 제1항에 따른 시책에는 다음 각 호의 사항이 포함되어야 한다.
 - 7의2. 정보통신망을 통하여 유통되는 정보 중 인공지능 기술을 이용하여 만든 거짓의 음향·화상 또는 영상 등의 정보를 식별하는 기술의 개발·보급

8. 「국가보안법」에서 금지하는 행위를 수행하는 내용의 정보
9. 그 밖에 범죄를 목적으로 하거나 교사(敎唆) 또는 방조하는 내용의 정보
- (추가예시) 00. 인공지능 기술을 이용하여 만든 거짓의 음향·화상 또는 영상 등의 정보임에도 워터마크를 통해 이에 해당함을 표시하지 아니한 정보**
- 제74조(벌칙)**
- ① 다음 각 호의 어느 하나에 해당하는 자는 1년 이하의 징역 또는 1천만원 이하의 벌금에 처한다.
1. 제8조제4항을 위반하여 비슷한 표시를 한 제품을 표시·판매 또는 판매할 목적으로 진열한 자
 2. 제44조의7제1항제1호를 위반하여 음란한 부호·문언·음향·화상 또는 영상을 배포·판매·임대하거나 공공연하게 전시한 자
 3. 제44조의7제1항제3호를 위반하여 공포심이나 불안감을 유발하는 부호·문언·음향·화상 또는 영상을 반복적으로 상대방에게 도달하게 한 자
- (추가예시) 0. 제44조의7 제1항 ()호를 위반하여 인공지능 기술을 이용하여 만든 거짓의 음향·화상 또는 영상 등의 정보임에도 워터마크를 통해 이에 해당하는 정보임을 표시하지 아니한 자**
4. 제50조제5항을 위반하여 조치를 한 자
 5. 삭제
 6. 제50조의8을 위반하여 광고성 정보를 전송한 자
 7. 제53조제4항을 위반하여 등록사항의 변경등록 또는 사업의 양도·양수 또는 합병·상속의 신고를 하지 아니한 자
- ② 제1항제3호의 죄는 피해자가 구체적으로 밝힌 의사에 반하여 공소를 제기할 수 없다.

한편, 정보통신망법 제44조의7 제2,3항은 방송통신위원회로 하여금 특정한 요건 하에서 제1항 각 호의 정보에 관하여 정보통신서비스 제공자 또는 게시판 관리·운영자로 하여금 그 처리를 거부·정지 또는 제한을 명할 수 있다고 규정하고 있는바, 워터마크가 표시되지 않은 덤페이크가 제44조의7 제1항 각 호 중 하나로 추가되는 경우 방송통신위원회에 의한 처리 거부·정지·제한 명령의 대상이 될 수 있을 것이다.

정보통신망 이용촉진 및 정보보호 등에 관한 법률

제44조의7(불법정보의 유통금지 등)

- ② 방송통신위원회는 제1항제1호부터 제6호까지, 제6호의2 및 제6호의3의 정보에 대

하여는 심의위원회의 심의를 거쳐 정보통신서비스 제공자 또는 게시판 관리·운영자로 하여금 그 처리를 거부·정지 또는 제한하도록 명할 수 있다. 다만, 제1항제2호 및 제3호에 따른 정보의 경우에는 해당 정보로 인하여 피해를 받은 자가 구체적으로 밝힌 의사에 반하여 그 처리의 거부·정지 또는 제한을 명할 수 없다.

③ 방송통신위원회는 제1항제7호부터 제9호까지의 정보가 다음 각 호의 모두에 해당하는 경우에는 정보통신서비스 제공자 또는 게시판 관리·운영자에게 해당 정보의 처리를 거부·정지 또는 제한하도록 명하여야 한다.

1. 관계 중앙행정기관의 장의 요청[제1항제9호의 정보 중 「성폭력범죄의 처벌 등에 관한 특례법」 제14조에 따른 촬영물 또는 복제물(복제물의 복제물을 포함한다)에 대하여는 수사기관의 장의 요청을 포함한다]이 있었을 것
2. 제1호의 요청을 받은 날부터 7일 이내에 심의위원회의 심의를 거친 후 「방송통신위원회의 설치 및 운영에 관한 법률」 제21조제4호에 따른 시정 요구를 하였을 것
3. 정보통신서비스 제공자나 게시판 관리·운영자가 시정 요구에 따르지 아니하였을 것

한편, 제44조의7 제2항에서는 방송통신위원회가 심의위원회의 심의를 거쳐¹²⁰⁾ 정보통신서비스 제공자 또는 게시판 관리·운영자로 하여금 그 처리를 거부·정지 또는 제한하도록 명할 수 있다고 규정하고 있는바, 덤페이크에 대한 심의위원회의 심의에 관하여 추가적으로 살펴볼 필요가 있다.

독립기구인 방송통신심의위원회는 방송통신위원회의 설치 및 운영에 관한 법률(이

120) 방송통신위원회의 시정명령 등 제재조치는 시정요구에 응하지 않는 사업자를 대상으로 방송통신심의위원회가 제재조치를 요청한 경우에 이루어진다.(정보통신에 관한 심의 규정 제17조)

정보통신에 관한 심의규정

제17조(제재조치) ① 위원회는 법 시행령 제8조제4항에 따라 정보통신서비스 제공자 또는 게시판 관리·운영자가 제15조에 따른 시정요구에 응하지 아니하는 경우로서 당해 정보가 정보통신망법 제44조의7제1항제1호부터 제6호까지의 불법정보에 해당하는 때에는 방송통신위원회에 다음 각 호의 사항을 포함하여 정보통신서비스 제공자 또는 게시판 관리·운영자로 하여금 그 취급거부·정지 또는 제한을 하도록 하는 명령을 하여 줄 것을 요청할 수 있다.

1. 위반사실
2. 제재조치의 종류
3. 그 밖에 필요한 사항

하 '방통위설치법') 제21조 및 동 시행령 제8조에 근거하여, 불법정보에 대한 사후심의 권한을 가진다. 이러한 통신심의제도는 사업자의 심의 요청, 이용자의 신고 등 민원접수, 자체 모니터링, 관계기관 요청 등 사전에 정해진 인지방법에 따라서만 심의 권한이 발동될 수 있다.

방송통신위원회 설치 및 운영에 관한 법률

제21조(심의위원회의 직무) 심의위원회의 직무는 다음 각 호와 같다.

4. 전기통신회선을 통하여 일반에게 공개되어 유통되는 정보 중 건전한 통신윤리의 함양을 위하여 필요한 사항으로서 대통령령으로 정하는 정보의 심의 및 시정요구

방송통신위원회의 설치 및 운영에 관한 법률 시행령

제8조(심의위원회의 심의대상 정보 등)

① 법 제21조제4호에서 "대통령령이 정하는 정보"란 정보통신망을 통하여 유통되는 정보 중 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제44조의7에 따른 불법정보 및 청소년에게 유해한 정보 등 심의가 필요하다고 인정되는 정보를 말한다.

② 법 제21조제4호에 따른 시정요구의 종류는 다음 각 호와 같다.

1. 해당 정보의 삭제 또는 접속차단
2. 이용자에 대한 이용정지 또는 이용해지
3. 청소년유해정보의 표시의무 이행 또는 표시방법 변경 등과 그 밖에 필요하다고 인정하는 사항

통신심의는 심의대상 인지 단계에서 개시된다. 이는 이용자의 신고, 자체 모니터링, 또는 타기관의 요청을 통하여 이루어진다. 인지된 심의대상은 확인 및 구분 절차를 거쳐 안전이 상정되는 심의부서의 검토 절차를 거친 후, 통신·권익보호특별위원회의 자문을 거쳐 통신심의소위원회 안전으로 상정되어 심의, 의결된다. 대부분 통신심의소 위원회에서 의결되나, 사안의 중대성 여하에 따라 전체회의에 상정될 수 있다.

방통위설치법 시행령 제8조 제2항에 따라, 정보통신망법 제44조의7에 해당하는 불법정보의 심의 결과를 근거로 정보통신서비스제공자 또는 게시판 관리·운영자에 대해 시정요구가 이루어진다. 방송통신심의위원회의가 행할 수 있는 시정요구의 종류로는

- ① 해당 정보의 삭제 또는 접속차단, ② 이용자에 대한 이용정지 또는 이용해지, ③

청소년유해정보의 표시의무 이행 등이 있다.

딥페이크 기술로 만든 영상임에도 워터마크를 표시하지 아니한 영상이 위 불법정보에 포함될 경우, 방송통신심의위원회는 ① 해당 정보의 삭제 또는 접속차단, ② 이용자에 대한 이용정지 또는 이용해지, ③ 딥페이크임을 나타내는 워터마크 표시의무 이행 등을 내용으로 시정요구할 수 있을 것이다.

그러나 방송통신위원회의 시정요구는 불법정보를 직접 생성한 이용자(개인)가 아니라, 정보통신서비스제공자 등 ‘사업자’를 매개로 이루어진다. 즉, 문제되는 불법정보를 웹상에서 지우도록 사업자에게 요청하여 더 이상의 유통을 차단하는 조치와, 불법정보 유통 이용자를 사업자가 제공하는 정보통신서비스에서 배제하는 유형의 두 가지 조치가 가능한데, 이 조치 모두 사업자를 매개해서만 가능하며, 불법정보 유통자, 제작자에게는 직접적으로 시정요구를 할 수 없는 한계가 있다¹²¹⁾.

3) 공직선거법 상 허위영상에 대한 워터마크 표시의무

딥페이크 기술로 만들어진 영상이 선거와 관련이 있는 경우 공직선거법 상 워터마크 표시의무를 추가하는 방안을 고려해볼 수 있다.

현행 공직선거법 제110조 제1항은 누구든지 선거운동을 위하여 후보자, 배우자 또는 직계존비속이나 형제자매의 출생지·가족관계·신분·직업·경력등·재산·행위·소속단체, 특정인 또는 특정단체로부터의 지지여부 등에 관하여 허위의 사실을 공표할 수 없으며, 공연히 사실을 적시하여 사생활을 비방할 수 없다고 규정하고 있으며, 제250조 제1항은 당선되거나 되게 할 목적으로 연설·방송·신문·통신·잡지·책·보·선전문서 기타의 방법으로 후보자에게 유리하도록 후보자, 후보자의 배우자 또는 직계존비속이나 형제자매의 출생지·가족관계·신분·직업·경력등·재산·행위·소속단체, 특정인 또는 특정단체로부터의 지지여부 등에 관하여 허위의 사실을 공표하

121) 이동후 외, 스마트 미디어 시대 인터넷 개인방송 규제 체계 정비, 국회입법조사처, 2016. 10., 제17면

거나 공표하게 한 자와 허위의 사실을 게재한 선전문서를 배포할 목적으로 소지한 자는 5년이하의 징역 또는 3천만원이하의 벌금에 처하고 있는바, 공직선거법 상의 규정은 주로 허위사실이라는 점에 초점을 두고 있다.

선거의 경우 선거기간이 상대적으로 단기간이고, 딥페이크 영상이 후보자 등에 대한 허위의 내용을 담고 있을 경우 그 파급력이 워낙 크기 때문에, 단순히 딥페이크에 워터마크를 심는 것에 그치지 않고 딥페이크로 인하여 변경된 내용이 무엇인지까지 표시해주어야 할 필요성이 높다. 이에 공직선거법 관련 내용은 아래의 변경내용 표시의무제도 부분에서 다시 한 번 살펴보도록 한다.

1.6. 결어

위에서 살펴본 바와 같이 영상의 제작자, 속성 등을 표시할 수 있는 식별혼적심기 방법 중 가장 도입가능성이 높은 것은 '디지털 워터마크' 표시의무제이다. 디지털 워터마크를 딥페이크 생성과정에 삽입하여 표시하는 것을 의무화한다면, 딥페이크 기술로 만들어진 영상임을 손쉽게 식별하고 가짜뉴스 등에 의한 피해확산을 방지할 수 있을 것이다.

국내에는 아직 딥페이크에 워터마크를 삽입할 의무에 관한 법령이나 법안이 없는 상황이며, 해외에서도 딥페이크에 워터마크를 삽입할 것을 요구하는 법이 시행되고 있지는 아니하고, 미국에서 법안의 형태로만 존재하고 있다. 국내법령에 딥페이크에 대한 워터마크 표시의무제를 도입한다면 정보통신망법 및 공직선거법에 표시의무제를 도입하는 것을 고려해볼 수 있다.

딥페이크에 워터마크 표시의무제도가 본격적으로 도입되는 경우 의무대상 영상의 범위를 법령에 구체적으로 특정하여 제시하여야 할 것이며, 구체적인 워터마크의 기술적인 사양이 제시되어야 할 것이다.

2. 딥페이크 변경내용 표시의무제도

가. 개념

'변경내용 표시의무제도'는 딥페이크 제작자에게 기존 영상에서 어떠한 내용이 변경되었는지 표시하여야 할 의무를 부여하여 시청자로 하여금 기존 영상에서 어떠한 내용이 변경되었는지 확인할 수 있도록 하는 제도이다.

변경내용 표시의무제도는 딥페이크에 디지털 워터마크를 표시하여 해당 영상이 딥페이크 기술로 제작된 영상이라는 점을 식별하도록 하는 것에서 나아가, 기존 영상에서 구체적으로 어떠한 내용을 변경했는지까지 표시하는데에 의의가 있다.

나. 변경내용 표시의무 관련 국내외 제도 및 입법현황

1) 국내의 경우

현재로서는 국내에 영상, 사진 등 콘텐츠와 관련하여, 변경내용 표시를 의무화하는 법 또는 제도가 없는 상황이다. 이는 딥페이크에 대하여도 마찬가지이다.

2) 해외의 경우

미국의 2019년 책임법에 따라 부당한 이용으로부터 유래한 허위의 외관으로부터 모든 사람들을 보호하기 위한 법률(Defending Each and Every Person from False Appearances by Keeping Exploitation Subject to Accountability Act of 2019)은 아직 본격적으로 시행되지는 아니하였으나, 해당 법안에서 딥페이크에 대한 변경내용 표시 의무를 부과하고 있어 살펴볼 필요가 있다.

위 법안은 ① 시각적 요소만을 포함하는 첨단 기술 허위 개인화 기록(advanced technological false personation record)의 경우, 시각적 요소가 지속되는 기간 동안 변경된 시각적 요소와 변경의 범위에 관한 간결한 설명이 나타나도록 영상 하단에 명확

하게 표시하여야 한다고 규정하고(SEC. 2 (d)), ② 청각적 요소만을 포함하는 첨단 기술 허위 개인화 기록(advanced technological false personation record)의 경우, 해당 기록이 포함하고 있는 변경된 청각적 요소와 변경의 범위에 관한 간결한 설명에 관하여 해당 기록의 시작 부분에서 명확하게 구두 설명을 하여야 한다고 규정하고 있다(SEC. 2 (e)).

즉 시각적, 청각적 요소를 포함하는 각 기록에 관하여, 해당 기록이 포함하고 있는 변경된 시각적·청각적 요소와 변경의 범위를 설명해야 할 의무를 부여하고 있는 것이다.

다음으로, 2020. 1. 16. 메릴랜드 주가 발표한 선거법-온라인 캠페인 자료-딥페이크 사용(Election Law-Online Campaign Material-Use of Deepfakes)¹²²⁾은 '딥페이크'를 "캠페인 자료에 관한 것이거나, 컴퓨터 생성 소프트웨어에 의해 강화 또는 변경되거나, 강화 또는 변경되지 않고 동작 묘사, 소리, 또는 발성을 묘사한 오디오 녹음·비디오 녹음·사진"이라고 정의하고(13-401.1(A).(2)), 선거일로부터 90일 이전에 온라인에 딥페이크를 게시·배포함으로써 유권자들이 특정 후보에 대하여 투표하는 것에 고의로 영향을 미치거나 미치려는 것을 금지하고 있다(13-401.1(C)(1)).

다만, 오디오 녹음, 비디오 녹화 또는 사진의 내용이 변경되었다는 정보 등 딥페이크에 대한 특정 정보를 명확하고 눈에 띄는 방식으로 공개한 경우에는 해당 조항이 적용되지 않는다고 규정하였다(13-401.1(C)(2)).

즉, 선거와 관련한 딥페이크에 관하여, 선거일로부터 90일 이전에 온라인에 딥페이크를 게시·배포하였더라도, 해당 오디오 녹음, 비디오 녹화 또는 사진의 내용이 변경되었다는 정보 등을 표시한 경우에는 법 위반이 되지 않도록 예외규정을 두고 있는 것이다.

다. 관계 법령 상 변경내용 표시의무제도 도입검토

122) 해당 법안에 관하여 2020. 2. 6. 청문회가 진행되었으나, 현재 기간만료로 폐기되었다.

위에서 딥페이크에 대한 워터마크 표시의무제도 도입에 관하여 살펴보았는바, 변경 내용 표시의무제도 도입검토 또한 같은 맥락에 있다.

딥페이크 변경내용 표시의무제도는 성폭력처벌법과 관련된 음란영상물에 관하여는 적용하기 적절하지 아니하며, 정보통신망법 상 불법정보, 공직선거법 상 허위영상물에 적용을 고려해볼 수 있다.

1) 정보통신망법 상 불법정보에 대한 변경내용 표시의무

딥페이크 변경내용 표시의무제를 시행하고 표시의무위반자에 대한 형사처벌 등 제재조항을 추가할 경우, 표시의무를 이행하지 않은 딥페이크 영상을 정보통신망법 제44조의7의 불법정보의 한 유형으로 보아 이를 제재할 수 있을 것이다.

다음은 딥페이크 변경내용 표시의무에 관하여 정보통신망법 제44조의7 제1항 각 호 및 제70조에 법문언을 추가하는 경우의 예시이다¹²³⁾.

정보통신망 이용촉진 및 정보보호 등에 관한 법률 제44조의7(불법정보의 유통금지 등)

① 누구든지 정보통신망을 통하여 다음 각 호의 어느 하나에 해당하는 정보를 유통하여서는 아니 된다.

(추가예시) 00. 인공지능 기술을 이용하여 만든 거짓의 음향·화상 또는 영상 등의 정보임에도 워터마크를 통해 이에 해당함을 표시하지 아니한 정보 및 변경된 내용을 표시하지 아니한 정보

제74조(벌칙)

① 다음 각 호의 어느 하나에 해당하는 자는 1년 이하의 징역 또는 1천만원 이하의 벌금에 처한다.

(추가예시) 0. 제44조의7 제1항 ()호를 위반하여 인공지능 기술을 이용하여 만든 거짓의 음향·화상 또는 영상 등의 정보임에도 워터마크를 통해 이에 해당하는 정보임을 표시하지 아니하거나, 변경된 내용을 표시하지 아니한 자

123) 제44조의7 제1항 아래의 추가되는 문구는 개정된 정보통신망법 제4조 제1항, 제2항 제7의2호 인공지능 기술 관련 시책에 사용된 법문언을 참조하였다.

정보통신망법 제44조의7 제2,3항은 방송통신위원회로 하여금 특정한 요건 하에서 제1항 각 호의 정보에 관하여 정보통신서비스 제공자 또는 게시판 관리·운영자로 하여금 그 처리를 거부·정지 또는 제한을 명할 수 있다고 규정하고 있는바, 변경내용이 표시되지 않은 딥페이크 영상이 제44조의7 제1항 각 호 중 하나로 추가되는 경우 방송통신위원회에 의한 처리 거부·정지·제한 명령의 대상이 될 수 있으며, 방송통신심의위원회는 심의를 통해 ① 해당 정보의 삭제 또는 접속차단, ② 이용자에 대한 이용정지 또는 이용해지, ③ 딥페이크 영상 중 변경된 부분을 표시하도록 하는 표시 의무 이행 등을 내용으로 시정요구할 수 있다.

2) 공직선거법 상 허위영상에 대한 변경내용 표시의무

딥페이크 기술로 만들어진 영상이 선거와 관련이 있는 경우 공직선거법 상 변경내용 표시의무를 부여하는 방안을 고려해볼 수 있다.

앞서 살펴본 바와 같이, 현행 공직선거법 제110조 제1항은 누구든지 선거운동을 위하여 후보자, 배우자 또는 직계존비속이나 형제자매의 출생지·가족관계·신분·직업·경력등·재산·행위·소속단체, 특정인 또는 특정단체로부터의 지지여부 등에 관하여 허위의 사실을 공표할 수 없으며, 공연히 사실을 적시하여 사생활을 비방할 수 없다고 규정하고 있으며, 제250조 제1항은 당선되거나 되게 할 목적으로 연설·방송·신문·통신·잡지·벽보·선전문서 기타의 방법으로 후보자에게 유리하도록 후보자, 후보자의 배우자 또는 직계존비속이나 형제자매의 출생지·가족관계·신분·직업·경력등·재산·행위·소속단체, 특정인 또는 특정단체로부터의 지지여부 등에 관하여 허위의 사실을 공표하거나 공표하게 한 자와 허위의 사실을 게재한 선전문서를 배포할 목적으로 소지한 자는 5년이하의 징역 또는 3천만원이하의 벌금에 처하고 있는바, 공직선거법 상의 규정은 주로 허위사실을 규제하는 것에 초점이 맞춰져 있다.

공직선거법 제110조(후보자 등의 비방금지)

① 누구든지 선거운동을 위하여 후보자, 배우자 또는 직계존비속이나 형제자매의 출생지·가족관계·신분·직업·경력등·재산·행위·소속단체, 특정인 또는 특정단체로부터의 지지여부 등에 관하여 허위의 사실을 공표할 수 없으며, 공연히 사실을 적시하여 사생활을 비방할 수 없다. 다만, 진실한 사실로서 공공의 이익에 관한 때에는 그러하지 아니하다.

② 누구든지 선거운동을 위하여 정당, 후보자, 후보자의 배우자 또는 직계존비속이나 형제자매와 관련하여 특정 지역·지역인 또는 성별을 공연히 비하·모욕하여서는 아니 된다.

제250조(허위사실공표죄)

① 당선되거나 되게 할 목적으로 연설·방송·신문·통신·잡지·책보·선전문서 기타의 방법으로 후보자에게 유리하도록 후보자, 후보자의 배우자 또는 직계존비속이나 형제자매의 출생지·가족관계·신분·직업·경력등·재산·행위·소속단체, 특정인 또는 특정단체로부터의 지지여부 등에 관하여 허위의 사실[학력을 게재하는 경우 제64조제1항의 규정에 의한 방법으로 게재하지 아니한 경우를 포함한다]을 공표하거나 공표하게 한 자와 허위의 사실을 게재한 선전문서를 배포할 목적으로 소지한 자는 5년이하의 징역 또는 3천만원이하의 벌금에 처한다.

② 당선되지 못하게 할 목적으로 연설·방송·신문·통신·잡지·책보·선전문서 기타의 방법으로 후보자에게 불리하도록 후보자, 그의 배우자 또는 직계존·비속이나 형제자매에 관하여 허위의 사실을 공표하거나 공표하게 한 자와 허위의 사실을 게재한 선전문서를 배포할 목적으로 소지한 자는 7년 이하의 징역 또는 500만원 이상 3천만원 이하의 벌금에 처한다.

딥페이크 영상의 경우 가공영상이라는 점에서 허위일 가능성이 높으나, 공직선거법에 딥페이크 기술을 이용하여 후보자 등에 관한 영상을 편집·합성 또는 가공하거나, 편집물·합성물·가공물 또는 복제물을 반포하는 자에 대해 원본 영상에서 변경된 내용을 표시하도록 의무를 부과하는 방안을 생각해볼 수 있으며, 미국 메릴랜드 주의 선거법-온라인 캠페인 자료-딥페이크 사용(Election Law-Online Campaign Material-Use of Deepfakes)¹²⁴⁾과 같이, 일단 딥페이크 영상의 제작 자체는 막지 않되, 내용이 변경되었다는 사실을 명확하고 눈에 띄는 방식으로 표시한 경우 면책하는 방법을 고려해볼 수 있다.

앞서 입법 개선 논의부분에서 살펴본 바와 같이, 현행 공직선거법에는 선거에 영향

124) 위 법안은 현재 기간만료로 폐기되었다.

을 미치려는 의도로 딥페이크 영상을 제작, 배포하거나, 딥페이크 영상을 제작하거나 배포함으로써 선거에 영향을 미치는 행위에 관한 별도의 규정이 없다.

이에 입법 개선 논의부분에서 선거에 영향을 미치려는 목적으로 딥페이크 영상을 제작, 배포하거나, 딥페이크 영상을 제작, 배포함으로써 결과적으로 선거에 영향을 미치는 행위에 대한 처벌규정의 신설을 고려할 필요가 있으며, 구체적으로, ㉠ 당선되거나 당선되지 못하게 할 목적으로 특정 후보자의 얼굴·신체 또는 음성을 대상으로 한 촬영물·영상물 또는 음성물을 편집·합성 또는 가공하여 유포하는 행위 자체를 처벌하는 조항, ㉡ 특정 후보자의 얼굴·신체 또는 음성을 대상으로 한 촬영물·영상물 또는 음성물을 편집·합성 또는 가공하여 유포함으로써 특정 후보자를 당선되거나 당선되지 못하게 한 행위를 처벌하는 조항을 신설하고, 딥페이크 영상을 통해 허위사실을 공표하는 행위는 기존 공직선거법 제250조를 통해 처벌함으로써, 딥페이크 기술 활용 허위 영상 등에 대한 처벌 공백을 해결하는 방향으로 공직선거법을 개정하는 방안을 제시한 바 있다.

입법 개선 논의 부분에서 검토한 내용은 특정 목적으로 딥페이크 영상을 아예 선거에 활용할 수 없도록 하고, 선거 관련 딥페이크 영상 중 허위의 경우에는 제250조에 의하여 처벌하도록 하는 것이었지만, 만약 공직선거법 상 딥페이크 영상 표시의무제 또는 변경내용 표시의무제가 도입되는 경우, 선거에도 딥페이크 영상이 활용될 수 있는 가능성이 열리게 되고, 변경내용 표시의무를 이행한 경우에는 면책되어 법적책임을 지지 않을 수 있게 된다.

위와 같이 공직선거법에 워터마크 표시의무제 또는 변경내용 표시의무제도를 도입할지의 여부는, 특정 목적으로 딥페이크 영상을 선거에 활용하는 것을 처음부터 허용할지 아니면 원천적으로 봉쇄할지 여부와 맞닿아 있는바, 이 부분에 대한 법령개선의 필요성 및 개선방향에 대한 관계부처 간 추가적인 논의가 필요할 것으로 보인다.

라. 결어

딥페이크 표시의무제도는 딥페이크 기술로 만든 영상이라는 점을 식별하도록 하는

데에 그치지만, 딥페이크 변경내용 표시의무제도는 어떠한 내용이 어떻게 변경되었는 지까지 확인할 수 있도록 하는 것으로, 딥페이크를 더욱 궁극적으로 규제하는 방안이며, 딥페이크로 인한 부작용을 더욱 감소시킬 수 있을 것으로 기대한다.

다만 워터마크 영상 표시의무제도와 마찬가지로, 도입될 경우 규제대상 영상의 범위와 기준이 법령에 구체적이고 명확히하게 설정되어야 할 것이며, 구체적인 워터마크 변경내용 표시에 관한 기술적인 사양이 제시되어야 할 것이다.

3. 기타 딥페이크에 대한 사후규제 방안

위에서 살펴본 워터마크 표시의무제도, 변경내용 표시의무제도 이외에 딥페이크에 대한 사후규제책으로서, 플랫폼 보류대기 시스템, 지정플랫폼의 운영 등을 검토해볼 수 있다.

위와 같은 플랫폼 보류대기 시스템, 지정플랫폼의 운영은 딥페이크 제작자가 딥페이크 영상이라는 사실을 표시하거나 공개하였을 경우에 적용이 가능하며, 그러한 표시의무제도가 도입되지 않을 경우 딥페이크 영상 제작자 또는 유통자에 의한 자율적 참여를 기대할 수 밖에 없다.

자율적 참여가 아니라면 딥페이크 제작자에 대한 강제적인 참여의무를 부과하여야 하는데, 이는 자칫 앞서 살펴본 딥페이크에 대한 사전허가제로 변질될 가능성이 있으므로 현실적인 도입이 어렵다.

딥페이크 제작자 또는 유통자가 플랫폼 보류대기 시스템, 지정플랫폼의 운영에 자발적으로 참여하지 않을 가능성이 큰바, 플랫폼 보류대기 시스템의 경우 결국 플랫폼 운영자가 자체적으로 개발한 딥페이크 식별기술을 활용하여 자체 모니터링을 하는 수 밖에 없으며, 지정플랫폼은 개설만 되고 실질적으로 사후규제책으로서의 역할을 하지 못할 가능성이 높다.

한편, 또한 보류대기 시스템을 도입하고 이를 정착시키기 위하여는 정부차원에서 식별기술을 보급하고 이를 적용할 의무를 부과하여야 할 것이나 아직까지 식별기술의 보급에 관한 대책 등이 진행되고 있지 않다. 딥페이크 식별기술이 보편화되어 있지

않은 상황 상 플랫폼 사업자에게 딥페이크 영상 업로드 시 이를 식별할 의무까지 부여하는 것은 어려워 보인다.

참고로 정보통신망법에는 플랫폼 운영자에게 특정 정보의 게시 전부터 이를 구분하거나 식별할 의무를 부과하는 조항은 없으며, 대부분 게시 이후 피해자의 요구에 의하여 또는 자체적인 판단에 의하여 삭제, 처리정지 등의 조치를 취하도록 되어있다.

이상과 같은 이유로 딥페이크에 대한 보류대기 시스템, 지정플랫폼의 운영의 도입은 현실적으로 어려워 보인다.

4. 결어

위에서 살펴본 바와 같이, 딥페이크에 대한 사후규제 방안으로는 딥페이크에 대한 워터마크 표시의무제도, 변경내용 표시의무제도의 도입 등이 있다. 위 제도는 정보통신망법 및 공직선거법 등에 반영을 고려해 볼 수 있다. 기타 사후규제 방안으로 딥페이크 영상에 대한 보류대기 시스템, 지정플랫폼의 운영을 생각해볼 수 있으나, 식별기술이 보편화되지 않은 현실 및 딥페이크 제작자의 자율적인 참여에 기대야하는 현실 상 위 제도의 도입은 어려워 보인다.

제4절 딥페이크 피해자의 구제강화 방안

1. 피해자의 삭제요구권 강화

딥페이크의 피해자는 개인정보보호법에 근거하여 개인정보처리자인 공공기관, 법인, 단체, 개인 등에 대하여 개인정보가 포함된 딥페이크 영상의 정정·삭제요구, 처리정지요구를 할 수 있다. 개인정보처리자는 위와 같은 정정·삭제요구, 처리정지요구를 받는 즉시 개인정보의 필요한 조치를 취하여야 한다(동법 제35조, 제36조).

개인정보보호법

제37조(개인정보의 처리정지 등)

- ① 정보주체는 개인정보처리자에 대하여 자신의 개인정보 처리의 정지를 요구할 수 있다. 이 경우 공공기관에 대하여는 제32조에 따라 등록 대상이 되는 개인정보파일 중 자신의 개인정보에 대한 처리의 정지를 요구할 수 있다.
- ② 개인정보처리자는 제1항에 따른 요구를 받았을 때에는 지체 없이 정보주체의 요구에 따라 개인정보 처리의 전부를 정지하거나 일부를 정지하여야 한다. 다만, 다음 각 호의 어느 하나에 해당하는 경우에는 정보주체의 처리정지 요구를 거절할 수 있다.
 1. 법률에 특별한 규정이 있거나 법령상 의무를 준수하기 위하여 불가피한 경우
 2. 다른 사람의 생명·신체를 해할 우려가 있거나 다른 사람의 재산과 그 밖의 이익을 부당하게 침해할 우려가 있는 경우
 3. 공공기관이 개인정보를 처리하지 아니하면 다른 법률에서 정하는 소관 업무를 수행할 수 없는 경우
 4. 개인정보를 처리하지 아니하면 정보주체와 약정한 서비스를 제공하지 못하는 등 계약의 이행이 곤란한 경우로서 정보주체가 그 계약의 해지 의사를 명확하게 밝히지 아니한 경우
- ③ 개인정보처리자는 제2항 단서에 따라 처리정지 요구를 거절하였을 때에는 정보주체에게 지체 없이 그 사유를 알려야 한다.
- ④ 개인정보처리자는 정보주체의 요구에 따라 처리가 정지된 개인정보에 대하여 지체 없이 해당 개인정보의 파기 등 필요한 조치를 하여야 한다.
- ⑤ 제1항부터 제3항까지의 규정에 따른 처리정지의 요구, 처리정지의 거절, 통지 등의 방법 및 절차에 필요한 사항은 대통령령으로 정한다.

개인정보보호법에 의한 딥페이크 영상의 정정·삭제요구, 처리정지요구는 내용과 상관없이 개인정보에 근거한 것이므로 딥페이크 영상의 피해자가 삭제를 요구하는 경우 특별한 사정이 없는 이상 즉시 삭제될 가능성이 높다.

한편, 딥페이크의 피해자는 해당 인터넷 게시판 운영자, SNS 운영자, 포털사이트 운영자, 어플리케이션 운영자 등 정보통신서비스 제공자에게 사생활 침해나 명예훼손 등 타인의 권리가 침해된 경우임을 주장하며 해당 영상의 삭제 또는 반박내용의 게재를 요청할 수 있다(제44조의2 제1항). 요청을 받은 정보통신서비스 제공자는 즉시 정보통신망법 상의 필요한 조치를 취하여야 한다(제44조의2 제2항).

정보통신망 이용촉진 및 정보보호 등에 관한 법률

제44조의2(정보의 삭제요청 등)

① 정보통신망을 통하여 일반에게 공개를 목적으로 제공된 정보로 사생활 침해나 명예훼손 등 타인의 권리가 침해된 경우 그 침해를 받은 자는 해당 정보를 처리한 정보통신서비스 제공자에게 침해사실을 소명하여 그 정보의 삭제 또는 반박내용의 게재(이하 “삭제등”이라 한다)를 요청할 수 있다.

② 정보통신서비스 제공자는 제1항에 따른 해당 정보의 삭제등을 요청받으면 지체 없이 삭제·임시조치 등의 필요한 조치를 하고 즉시 신청인 및 정보게재자에게 알려야 한다. 이 경우 정보통신서비스 제공자는 필요한 조치를 한 사실을 해당 게시판에 표시하는 등의 방법으로 이용자가 알 수 있도록 하여야 한다.

제2조(정의)

① 이 법에서 사용하는 용어의 뜻은 다음과 같다.

1. "정보통신망"이란 「전기통신사업법」 제2조제2호에 따른 전기통신설비를 이용하거나 전기통신설비와 컴퓨터 및 컴퓨터의 이용기술을 활용하여 정보를 수집·가공·저장·검색·송신 또는 수신하는 정보통신체제를 말한다.

그런데 정보통신망법 제44조의2 제1항은 사생활 침해나 명예훼손 등 타인의 권리가 침해된 경우 그 침해를 받은 자가 침해사실을 소명할 것을 요구하고 있어, 딥페이크 영상이 사생활 침해나 명예훼손과 관련이 없는 경우에는 삭제요구를 할 수 없도록 되어 있다.

따라서 딥페이크의 피해자가 정보통신서비스 제공자에게 해당 영상의 삭제를 요청한다고 하더라도 해당 영상이 사생활 침해나 명예훼손 등과 관련이 없다는 이유로 삭제를 거절당할 가능성이 있다.

그러나 딥페이크 영상이 피해자의 의사에 반하여 제작된 경우, 해당 영상은 피해자의 인격적인 부분과도 관련이 있으므로, 딥페이크 영상의 내용이 사생활침해나 명예훼손 등과 관련이 없는 경우라도 하더라도 이에 대한 삭제를 요구할 권리를 부여하는 것이 바람직하다.

딥페이크 영상의 경우 사생활침해 또는 명예훼손과 관련이 없다고 하더라도, 피해자의 의사에 반하여 제작되거나 배포된 영상이라는 이유만으로 정보통신서비스 제공자에게 영상의 즉시삭제를 요청할 수 있는 권리를 부여하여, 딥페이크피해자의 권리를 더욱 강하게 보호할 필요성이 있다.

만약 딥페이크 영상이라는 이유만으로 즉시 삭제를 요구할 수 있는 권리를 인정한다면, 아래와 같은 형식으로 정보통신망법 제44조의2 제1항에 추가가 가능할 것으로 보인다.

정보통신망 이용촉진 및 정보보호 등에 관한 법률

제44조의2(정보의 삭제요청 등)

(개정예시) ① 누구든지 다음 각 호의 정보를 처리하는 정보통신서비스 제공자에게 해당 실을 소명하여 그 정보의 삭제 또는 반박내용의 게재(이하 “삭제등”이라 한다)를 요청할 수 있다.

1. 정보통신망을 통하여 일반에게 공개를 목적으로 제공된 정보로 사생활 침해나 명예훼손 등 타인의 권리가 침해된 경우

2. **딥페이크 기술을 활용한 정보로 요청자의 의사에 반하여 생성되거나 유통된 경우**

딥페이크에 대한 표시의무제도가 시행되는 경우 피해자와 정보통신서비스 제공자 모두 곧바로 딥페이크 기술이 활용된 영상임을 식별할 수 있으므로, 피해자의 삭제요구를 받으면 즉시 삭제될 수 있을 것으로 기대한다.

2. 국내대리인 지정 제도의 활용

가. 국내대리인 지정 제도의 개념

해외 인터넷 기업에게 개인정보보호를 위해 국내대리인을 두도록 의무를 부여하는 정보통신망법 제32조의5 규정이 2018. 9. 18. 신설되었고, 위 정보통신망법에서 위임한 국내대리인 지정 의무 대상자의 기준을 정하기 위한 동법 시행령 개정안이 2019. 3. 19. 시행됨에 따라 국내대리인 지정 의무가 국내에 정식으로 도입되었다.

당초 국내대리인제도는 정보통신망법 개정으로 도입되었으나, 정보통신망법에 규정되어 있던 개인정보 보호 관련 규정이 개인정보보호법으로 일원화됨에 따라, 개인정보보호법 제39조의11이 신설되어, 개인정보보호법의 규율 하에 시행되고 있다.

개인정보보호법

제39조의11(국내대리인의 지정)

① 국내에 주소 또는 영업소가 없는 정보통신서비스 제공자등으로서 이용자 수, 매출액 등을 고려하여 대통령령으로 정하는 기준에 해당하는 자는 다음 각 호의 사항을 대리하는 자(이하 "국내대리인"이라 한다)를 서면으로 지정하여야 한다.

1. 제31조에 따른 개인정보 보호책임자의 업무
2. 제39조의4에 따른 통지·신고
3. 제63조제1항에 따른 관계 물품·서류 등의 제출

제31조(개인정보 보호책임자의 지정)

② 개인정보 보호책임자는 다음 각 호의 업무를 수행한다.

1. 개인정보 보호 계획의 수립 및 시행
2. 개인정보 처리 실태 및 관행의 정기적인 조사 및 개선
3. 개인정보 처리와 관련한 불만의 처리 및 피해 구제
4. 개인정보 유출 및 오용·남용 방지를 위한 내부통제시스템의 구축
5. 개인정보 보호 교육 계획의 수립 및 시행
6. 개인정보파일의 보호 및 관리·감독
7. 그 밖에 개인정보의 적절한 처리를 위하여 대통령령으로 정한 업무

국내대리인 제도는 국내에 주소 또는 영업소가 없는 해외 정보통신서비스 제공자로서 이용자수, 매출액 등을 고려하여 대통령령으로 정하는 기준에 해당하는 자로 하여금, 개인정보보호법 제31조에 따른 개인정보 보호책임자의 업무를 수행하도록 하는 것이다.

개인정보보호법 제31조에서는 개인정보 보호책임자를 지정하도록 하면서, 개인정보 보호책임자의 업무범위로 개인정보 처리와 관련된 불만의 처리 및 피해구제에 관하여 규정하고 있다.

나. 적용 및 한계점

앞서 본 바와 같이 딥페이크의 피해자는 개인정보보호법 및 정보통신망법에 근거하여 영상의 정정·삭제, 처리정지 등을 요구할 권리가 있다. 개인정보처리자 또는 정보통신서비스 제공자는 위와 같은 요청을 받는 경우 즉시 필요한 조치를 취하여야 한다. 위 업무는 개인정보보호법 제31조의 개인정보 처리와 관련된 불만의 처리 및 피해구제 업무에 속한다고 볼 수 있다.

해외 인터넷사업자가 위와 같은 개인정보 처리와 관련된 불만의 처리 및 피해구제 업무를 제대로 처리하지 않을 경우, 개인정보보호법 제64조에 따른 시정조치 또는 제75조에 따른 과태료 부과대상이 된다. 2020. 9. 개인정보보호위원회는 제3회 위원회 회의에서 국내대리인 제도를 부실하게 운영한 해외 사업자 7곳에 개선권고를 의결한 바 있다.

위와 같이 딥페이크로 인한 피해자는 현행 개인정보보호법 상 국내대리인제도를 통하여 해외사업자에게 개인정보 처리와 관련한 불만의 처리 및 피해 구제로서 영상의 정정·삭제, 처리정지 등을 요청할 수 있다.

그러나 국내대리인 제도의 경우 개인정보 처리와 관련된 불만의 처리 및 피해구제 업무를 하는 개인정보 보호책임자를 지정하도록 하는 것에 그치고 있어, 지정된 책임자가 있다고 하더라도 실제로 업무를 하도록 강제할 수 있는 방법이 없다.

또한 딥페이크의 경우, 특히 음란물의 경우에 해외 소규모 플랫폼을 통한 피해가 발생하는 경우가 많은데, 국내대리인의 지정요건은 아래와 같이 전년도 매출액 1조원 이상, 정보통신서비스 부문 전년도 매출액 100억원 이상 등 규모가 큰 사업자를 대상으로 하고 있어, 해외 소규모 정보통신서비스 제공자는 국내대리인 지정제도의 대상이 아니다.

개인정보 보호법 시행령

제48조의9(국내대리인 지정 대상자의 범위)

① 법 제39조의11제1항 각 호 외의 부분에서 "대통령령으로 정하는 기준에 해당하는 자"란 다음 각 호의 어느 하나에 해당하는 자를 말한다.

1. 전년도(법인인 경우에는 전 사업연도를 말한다) 매출액이 1조원 이상인 자
 2. 정보통신서비스 부문 전년도(법인인 경우에는 전 사업연도를 말한다) 매출액이 100억원 이상인 자
 3. 전년도 말 기준 직전 3개월간 그 개인정보가 저장·관리되고 있는 이용자 수가 일일평균 100만명 이상인 자
 4. 이 법을 위반하여 개인정보 침해 사건·사고가 발생하였거나 발생할 가능성이 있는 경우로서 법 제63조제1항에 따라 관계 물품·서류 등 자료의 제출을 요구받은 자
- ② 제1항제1호 및 제2호에 따른 매출액은 전년도(법인인 경우에는 전 사업연도를 말한다) 평균환율을 적용하여 원화로 환산한 금액을 기준으로 한다.

이처럼 국내대리인 제도 지정 의무는, 전년도 매출액(1조원), 전년도 말 기준 개인정보가 저장, 관리되고 있는 이용자 수(100만명) 등 일정한 규모 이상의 해외 인터넷 사업자만을 그 수범자로 한다는 점, 국내대리인의 역할은 개인정보 보호책임자를 ‘대리’하는 것이지 개인정보 보호책임자 자체는 아니므로 해외 사업자와 이용자 사이에 체결되는 세부적인 계약 내용에 따라 업무 범위가 달라질 수 있다는 점¹²⁵⁾, 국내대리인 미지정에 따른 과태료가 2천만원 이하로 규정되어 있어 행정벌이 매우 경미하다는 점, 개인정보보호위원회는 국내대리인 제도 운영을 소홀히 한 해외사업자에게 시정조치를 할 권한을 보유하고 있으나 벌칙 이나 과징금 등 제도 운영의 실효성을

125) 방송통신위원회, 국내대리인 지정제도 안내서, 제3면

강제할 수 있는 제재수단을 부과할 권한이 없다는 점 등의 한계가 있다.

이러한 연유로 해외 인터넷 사업자가 제공하는 플랫폼 내에서 권리를 침해당한 딥페이크 피해자는 사실상 권리보호 수단이 없게 되는 권리보호의 사각지대의 놓이게 된다.

딥페이크는 해외 소규모 정보통신서비스 제공자에 의하여 피해가 발생하는 경우가 많은바, 피해자의 구제강화를 위하여 국내대리인 지정 제도의 기준을 낮추는 방향으로 조정하는 것을 고려해볼 수 있다.

3. 결어

딥페이크 피해자의 구제강화 방안으로 딥페이크 피해자의 삭제요구권 강화, 국내대리인 지정제도의 활용을 고려해볼 수 있다.

현행 정보통신망법 상 삭제요구권 행사시 사생활 침해나 명예훼손 등 타인의 권리가 침해된 경우 그 침해를 받은 자가 침해사실을 소명할 것을 요구하고 있으나(정보통신망법 제44조의2 제1항), 해당 콘텐츠가 딥페이크 기술에 의하여 제작된 영상이라는 점만을 소명하면 곧바로 삭제요청을 할 수 있도록 삭제요구권의 적용범위를 확대하여 피해자의 구제를 강화할 수 있다. 위 삭제요구권의 강화방안이 딥페이크 표시의 무제도와 함께 시행된다면 더욱 효과적인 피해자 구제가 이루어질 수 있다.

한편, 딥페이크의 피해자는 해외 정보통신서비스 제공자에 대한 국내대리인 지정제도를 활용하여, 지정된 개인정보보호책임자에게 해당 영상에 불만의 처리 및 피해구제업무를 요청할 수 있다. 다만 딥페이크의 특성상 해외 소규모 정보통신서비스 제공자에 의한 피해가 많은바, 국내대리인 지정 제도의 지정요건을 낮추어 피해자의 구제를 더욱 강화할 필요성이 있다.

제5절 딥페이크 식별 기술의 지원

1. 서설

위에서 딥페이크에 대한 사전규제 방안, 사후규제 방안, 피해자 구제강화 방안 등에 관하여 살펴보았다. 위와 같은 방안은 전부 딥페이크로 인한 사회적인 부작용을 줄이기 위한 것이나, 기본적으로 위 방안들이 실효성 있게 도입되기 위하여는 딥페이크 식별 기술이 뒷받침 되어야 한다.

앞서 딥페이스 기술동향에서 살펴본 바와 같이 딥페이크를 식별하는 기술 또한 생성기술과 함께 발전하는 중이기는 하나, 딥페이크 생성을 통한 이윤창출의 효과가 워낙 크고 막강하기 때문에 딥페이크를 검출 및 해결하기 위한 기술의 발전이 늘 후행할 수밖에 없다. 또한 딥페이크 기술은 데이터를 조작하고자 하는 사람이 새로운 기술을 개발하여 어느 정도 성과를 거둔 후에야 비로소 검출 문제를 해결하기 위한 여건이 조성되는 특성이 있다.

따라서 정부에서 의무적으로, 민간차원에서 자발적으로 딥페이크를 식별하기 위한 지원하여야 할 필요성이 높다.

이하에서는 딥페이크 식별 기술의 지원현황, 딥페이크 식별 인증기관의 지정 또는 설립, 딥페이크 식별 기술 지원방안 등에 관하여 살펴보면서 해당 내용을 관련 법령에 어떻게 반영할지에 관하여 검토하도록 한다.

2. 딥페이크 식별 및 인증을 위한 기관 지정 또는 설립 근거규정 마련

가. 기존의 논의

딥페이크로 인한 부작용을 줄이기 위한 여러 방안들은 기본적으로 딥페이크 식별

기술의 뒷받침을 전제로 하고 있다. 현실여건 상 도입이 어렵다고 보이는 딥페이크 영상 보류대기 시스템 등도 딥페이크 식별 기술이 뒷받침 된다면 실행될 수 있는 여지가 있다.

딥페이크 식별기술은 딥페이크 생성기술에 비하여 발전동력이 약하고 민간주도에 의해 진행되는 것을 기대하기 쉽지 않다. 따라서 정부차원에서 딥페이크 식별 및 인증을 위한 기관을 별도로 지정하여 운영할지에 관한 논의가 필요하다. 아직까지 딥페이크 식별기술 및 딥페이크 인증을 위한 구체적인 제도가 추진되고 있는 것이 없기 때문에, 그러한 제도를 효과적으로 정착시키고 발전시키기 위한 별도 기관에 관한 논의도 활발하지 않은 상황이다.

2019. 11. 15. 박광온의원 등 10인에 의하여 방송통신발전 기본법 일부개정 법률안이 발의되었는데(의안번호 2023823), 해당 개정법률안에서는 방송통신콘텐츠의 사실 여부를 객관적으로 확인하는 활동을 하는 기관·법인 또는 단체에 대한 인증업무를 수행하는 인증기구에 기금을 지원할 수 있도록 하는 내용, 콘텐츠 조작여부를 찾아낼 수 있는 인공지능형 로봇 연구개발 사업, 안 제19조의2에 따른 인증기구에 대한 지원, 건전하고 신뢰성 있는 방송통신서비스 지원 사업을 방송통신발전기금의 용도로 규정하도록 하는 내용을 담고 있었다.

위 개정안 제19조의2의 방송통신콘텐츠의 사실 여부를 객관적으로 확인하는 활동에는 딥페이크 기술로 제작된 콘텐츠의 사실 여부를 확인하는 활동이 포함되고, 개정안 제26조 제1항 제1호의 조작된 방송통신콘텐츠를 찾아내기 위한 인공지능형 로봇 등에 관한 연구개발 사업에는 인공지능 기술에 기반한 딥페이크를 식별하기 위한 연구개발 사업이 포함되는바, 위 개정안은 결국 딥페이크 식별 및 인증 지원을 위한 법률안이였다.

구체적으로 방송통신발전 기본법 제19조의2 신설제안은, 최근 인공지능(AI)을 이용한 딥페이크 기술 등을 사용하여 허위의 조작된 방송통신콘텐츠 등을 통하여 사실이 왜곡되거나 과장되어 전파되는 사례가 빈번하게 발생하고 있으며, 이로 인해 방송통신콘텐츠 등의 내용에 대한 사실여부를 확인하기 위한 비영리기관 또는 단체가 생겨

나는 등 정확한 사실전달을 위한 움직임이 일어나고 있으나, 재정적인 어려움으로 인하여 운영에 어려움을 겪고 있는 상황이며, 국가차원에서도 방송통신콘텐츠의 조작여부를 찾아낼 수 있는 인공지능형 로봇 등에 관한 연구개발 투자가 저조한 실정이라는 점, 이에 시청자와 이용자의 권익을 보호하기 위한 사업을 수행하는 기관·법인 또는 단체에 대한 인증업무를 수행하는 민간 자율 팩트체크 인증기구에 기금을 지원할 수 있도록 법적 근거를 마련하고, 지원을 받은 인증기구는 기금을 시청자와 이용자의 권익을 보호하기 위한 사업을 수행하는 것으로 인증 받은 기관·법인 또는 단체에 지원하도록 하는 한편, 방송통신발전기금의 용도에 방송통신콘텐츠의 조작여부를 찾아낼 수 있는 인공지능형 로봇 등에 관한 연구개발 사업을 명시하여 방송통신콘텐츠의 사실 확인을 위한 연구개발 투자를 강화할 필요가 있다는 점을 지적하며 이루어졌다.

방송통신발전 기본법 일부개정 법률안

제19조의2(인증기구에 대한 지원)

- ① 과학기술정보통신부장관과 방송통신위원회는 시청자와 이용자의 권익을 보호하기 위한 활동(수정의견 : 방송통신콘텐츠의 사실 여부를 객관적으로 확인하는 활동)을 하는 기관·법인 또는 단체에 대한 인증업무를 수행하는 인증기구에 기금을 지원할 수 있다.
- ② 제1항에 따른 지원을 받으려는 인증기구는 다음 각 호의 요건을 모두 갖추어야 한다.
 1. 비영리 목적의 기관·법인 또는 단체
 2. 객관적인 인증 기준 방법 및 절차
 3. 그 밖에 대통령령으로 정하는 요건
- ③ 제1항에 따라 예산(수정의견 기금)을 지원받은 인증기구는 그 예산(수정의견 기금)을 시청자와 이용자의 권익을 보호하기 위한 활동(수정의견 : 방송통신콘텐츠의 사실 여부를 객관적으로 확인하는 활동) 목적으로 인증 받은 기관·법인 또는 단체에 대하여 지원하는 용도로 사용하여야 한다.
- ④ 과학기술정보통신부장관과 방송통신위원회는 제1항에 따라 예산(수정의견 기금)을 지원받은 인증기구의 활동과 운영에 있어서 독립성과 자율성을 보장하여야 한다.
- ⑤ 제1항에 따라 예산을 지원받은 인증기구는 대통령령으로 정하는 바에 따라 기금사용결과를 연 1회 과학기술정보통신부장관과 방송통신위원회에 보고하여야 한다.
- ⑥ 제1항부터 제5항까지의 규정에 따른 인증기구의 지원(수정의견 인증기구에 대한 지원) 등에 필요한 기준·방법 및 절차 등에 관한 사항은 대통령령으로 정한다.

또한 방송통신발전 기본법 제26조의 개정제안은, 콘텐츠 조작여부를 찾아낼 수 있는 인공지능형 로봇 연구개발 사업, 안 제19조의2에 따른 인증기구에 대한 지원, 건전하고 신뢰성 있는 방송통신서비스 지원 사업을 방송통신발전기금의 용도로 규정하려는 목적으로 이루어졌다.

<표 4-2> 방송통신발전 기본법 제26조 개정안

현 행	개 정 안
제26조(기금의 용도) ① 기금은 다음 각 호의 어느 하나에 해당하는 사업에 사용된다. 1. 방송통신에 관한 연구개발 사업 2. ~ 5의2. (생략) <신설> <신설> 6. ~ 16. (생략) ② ~ ④ (생략)	제26조(기금의 용도) ① 기금은 다음 각 호의 어느 하나에 해당하는 사업에 사용된다. 1. 방송통신에 관한 연구개발 사업 <u>(조작된 방송통신콘텐츠를 찾아내기 위한 인공지능형 로봇 등에 관한 연구개발 사업을 포함한다)</u> 2. ~ 5의2. (현행과 같음) <u>5의3. 제19조의2에 따른 인증기구에 대한 지원</u> <u>5의4. 건전하고 신뢰성 있는 방송통신서비스 지원 사업</u> 6. ~ 16. (현행과 같음) ② ~ ④ (현행과 같음)

현행 방송통신발전 기본법 제24조는 과학기술정보통신부장관과 방송통신위원회가 방송통신의 진흥을 지원하기 위하여 방송통신발전기금을 설치한다고 되어 있는바, 위 개정안 제26조 제1항은 위 기금의 용도로 조작된 방송통신콘텐츠를 찾아내기 위한 인공지능형 로봇 등에 관한 연구개발 사업(제26조 제1항 1호), 시청자와 이용자의 권익을 보호하기 위한 활동(수정의견 : 방송통신콘텐츠의 사실 여부를 객관적으로 확인하는 활동)을 하는 기관·법인 또는 단체에 대한 인증업무를 수행하는 인증기구에 대한 지원(제26조 제1항 5의3호), 건전하고 신뢰성 있는 방송통신서비스 지원사업(제26조

제1항 5의4호)을 추가한 것이었다.

만약 위 법률안이 통과되었다면 딥페이크 식별 및 인증업무를 담당하는 기관에 대한 재원이 마련됨에 따라 인증기구 지정 및 운영에 대한 논의가 본격적으로 진행되었을 가능성이 있다.

그러나 위 방송통신발전 기본법 일부개정 법률안은 국회 임기만료로 결국 폐기되었으며, 현재 동일한 취지의 법률안이 다시 발의되어 있지는 않은 것으로 확인된다.

딥페이크 식별 및 인증을 위한 별도의 전담기구 운영은 딥페이크 기술의 확산 및 피해자의 확대가 예상됨에 따라 반드시 추가적인 논의가 필요한 부분이다. 따라서 현재 관련 법률 및 법률안이 없다고 하더라도 딥페이크 관련 총괄 전담부서의 지휘 아래 꾸준히 관심을 가지고 운영 논의가 지속되어야 할 것으로 보인다.

나. 정보통신망법 상 딥페이크 식별 및 인증을 위한 기관 근거규정 마련

1) 서설

위에서 방송통신발전 기본법 개정안에 담겨있었던 딥페이크 식별 및 인증을 위한 별도 기관에 관한 내용을 살펴보았다. 기본적으로 방송통신발전 기본법은 방송통신의 공익성, 공공성을 보장하고 방송통신 발전을 위하여 제정된 법이다(방송통신발전 기본법 제1조).

반면, 정보통신망법은 정보통신서비스를 이용하는 자를 보호하고 정보통신망을 건전하고 안전하게 이용할 수 있는 환경을 조성하는 것을 목적으로 한다(정보통신망법 제1조). 또한 딥페이크 표시의무, 표시내용 변경의무 등의 내용을 입법화하는 경우 정보통신망법에 이를 반영하는 것이 적절한바, 딥페이크 식별 및 인증을 위한 별도 기관의 설립 또는 운영에 관한 내용을 법제화하는 경우, 방송통신발전 기본법 보다는 입법목적에 정보통신망 이용자 보호 취지에 포함되고, 딥페이크와 관련된 조항이 이미 있는 정보통신망법에 이를 반영하는 것이 더욱 적절하다.

이하에서는 정보통신망법에 딥페이크 식별 및 인증을 위한 별도 기관의 지정 및 설

립에 관한 근거규정을 어떻게 반영하여야 할지에 관하여 검토하고자 한다.

2) 정보통신망법 상 인증기관 지정 근거규정 마련

최근 개정된 정보통신망법(2020. 6. 29. 공포, 2020. 12. 10. 시행)은 과학기술정보통신부장관 또는 방송통신위원회로 하여금 정보통신망을 통하여 유통되는 정보 중 인공지능 기술을 이용하여 만든 거짓의 음성·화상 또는 영상 등의 정보를 식별하는 기술의 개발·보급에 관한 시책을 마련할 것을 규정하고 있다(제4조 제1항, 제2항 제7의2호). 딥페이크는 인공지능 기술을 이용하여 만든 거짓의 음성·화상 또는 영상 등의 정보에 해당하되, 딥페이크 관련 시책마련에 관한 조항이라고 할 수 있다. 그러나 아직 구체적인 시책이 마련되어 있지는 않은 상황이며, 딥페이크 식별 및 인증을 위한 기관에 관한 내용도 신설되어 있지 않다.

정보통신망법에서는 정보통신망법 제4조 제2항 시책과 관련하여 여러 규정을 두고 있는바, 그 중 인증기관 지정에 관한 내용을 담고 있는 것들이 있다.

정보통신망법 제9조 제1항에서는 과학기술정보통신부장관이 제8조 제1항 본문에 따라 고시된 표준에 적합한 제품임을 '인증하는 기관'을 지정할 수 있다고 규정하고 있고, 동법 제47조 제6항에서는 과학기술정보통신부장관이 한국인터넷진흥원 또는 과학기술정보통신부장관이 '지정하는 기관'으로 하여금 동조 제1항 및 제2항에 따른 '인증에 관한 업무'를 수행하게 할 수 있다고 규정하고 있으며, 제7항에서는 과학기술정보통신부장관이 인증에 관한 업무를 효율적으로 수행하기 위하여 필요한 경우 '인증심사 업무를 수행하는 기관'을 지정할 수 있다고 규정하고 있다.

<표 4-3> 정보통신망법 제4조 제2항 시책 관련 규정 중 기관 지정 관련 규정

정보통신망법 제4조 제2항 시책	관 련 조 항
2. 정보통신망의 표준화	제8조(정보통신망의 표준화 및 인증) ① 과학기술정보통신부장관은 정보통신망의 이용을 촉진하기

	위하여 정보통신망에 관한 표준을 정하여 고시하고, 정보통신 서비스 제공자 또는 정보통신망과 관련된 제품을 제조하거나 공급하는 자에게 그 표준을 사용하도록 권고할 수 있다. 다만, 「산업표준화법」 제12조에 따른 한국산업표준이 제정되어 있는 사항에 대하여는 그 표준에 따른다. 제9조(인증기관의 지정 등) ① 과학기술정보통신부장관은 정보통신망과 관련된 제품을 제조하거나 공급하는 자의 제품이 제8조제1항 본문에 따라 고시된 표준에 적합한 제품임을 <u>인증하는 기관(이하 “인증기관”이라 한다)을 지정할 수 있다.</u> ③ 제1항 및 제2항에 따른 인증기관의 지정기준·지정절차, 지정취소·업무정지의 기준 등에 필요한 사항은 과학기술정보통신부령으로 정한다.
7의2. 정보통신망을 통하여 유통되는 정보 중 인공지능 기술을 이용하여 만든 거짓의 음향·화상 또는 영상 등의 정보를 식별하는 기술의 개발·보급	관련 규정 없음
8. 정보통신망의 안전성 및 신뢰성 제고	제47조(정보보호 관리체계의 인증) ① 과학기술정보통신부장관은 정보통신망의 안정성·신뢰성 확보를 위하여 관리적·기술적·물리적 보호조치를 포함한 종합적 관리체계(이하 “정보보호 관리체계”라 한다)를 수립·운영하고 있는 자에 대하여 제4항에 따른 기준에 적합한지에 관하여 인증을 할 수 있다. ⑥ 과학기술정보통신부장관은 <u>한국인터넷진흥원 또는 “과학기술정보통신부장관이 지정한 기관(이하 “정보보호 관리체계 인증기관”이라 한다)으로 하여금 제1항 및 제2항에 따른 인증에 관한 업무로서 다음 각 호의 업무를 수행하게 할 수 있</u>

	다. 1. 인증 신청인이 수립한 정보보호 관리체계가 제4항에 따른 인증기준에 적합한지 여부를 확인하기 위한 심사(이하 "인증심사"라 한다) 2. 인증심사 결과의 심의 3. 인증서 발급·관리 4. 인증의 사후관리 5. 정보보호 관리체계 인증심사원의 양성 및 자격관리 6. 그 밖에 정보보호 관리체계 인증에 관한 업무 ⑦ 과학기술정보통신부장관은 <u>인증에 관한 업무를 효율적으로 수행하기 위하여 필요한 경우 인증심사 업무를 수행하는 기관(이하 "정보보호 관리체계 심사기관"이라 한다)을 지정할 수 있다.</u> 제48조의5(정보통신망연결기기등 관련 침해사고의 대응 등) ④ <u>과학기술정보통신부장관은 대통령령으로 정하는 전문기관이 다음 각 호의 사업을 수행하는 데 필요한 비용을 지원할 수 있다.</u> 1. 정보통신망연결기기등과 관련된 정보보호지침 마련을 위한 연구 2. 정보통신망연결기기등과 관련된 시험·검사·인증 등의 기준 개선 연구
--	--

위와 같이 정보통신망법에서는 인증업무를 하는 기관을 지정하도록 하는 규정을 두고 있는바, 동법 제4조 제2항 제7조의2의 정보통신망을 통하여 유통되는 정보 중 인공지능 기술을 이용하여 만든 거짓의 음성·화상 또는 영상 등의 정보를 식별하고 하는 이를 인증하는 기관의 지정에 관하여도 같은 방식으로 조항을 신설하면 될 것으로 보인다.

딥페이크 식별 및 인증을 위한 기관의 지정 근거는 다음과 같은 방식으로 마련할 수 있으며, 아래와 같은 신설조항의 위치는 정보통신망법 제4조 시책과 관련된 조항들이 포진해있는 동법 제5조 내지 제15조 근방으로 하는 것이 적절해 보인다.

정보통신망 이용촉진 및 정보보호 등에 관한 법률
(신설예시) 제00조(인공지능 기술을 이용한 거짓 정보의 식별 및 인증)

- ① (과학기술정보통신부장관/방송통신위원회/정부¹²⁶)는 정보통신망을 통하여 유통되는 정보 중 인공지능 기술을 이용하여 만든 거짓의 음향·화상 또는 영상 등의 정보를 식별하고 이를 인증하는 기관을 지정할 수 있다.
- ③ 제1항에 따른 인증기관의 지정기준·지정절차, 지정취소·업무정지의 기준 등에 필요한 사항은 (과학기술정보통신부령/대통령령)¹²⁷으로 정한다.

3) 정보통신망법 상 기관 설립 근거규정 마련

한편, 정보통신망법에서 기관의 설립에 관한 근거규정을 두고 있는 것은 제52조의 한국인터넷진흥원이 유일하다.

제52조(한국인터넷진흥원)

- ① 정부는 정보통신망의 고도화(정보통신망의 구축·개선 및 관리에 관한 사항은 제외한다)와 안전한 이용 촉진 및 방송통신과 관련한 국제협력·국외진출 지원을 효율적으로 추진하기 위하여 한국인터넷진흥원(이하 "인터넷진흥원"이라 한다)을 설립한다.
- ② 인터넷진흥원은 법인으로 한다.
- ③ 인터넷진흥원은 다음 각 호의 사업을 한다.
- (각호 생략)

마찬가지로 동법 제4조 제2항 제7조의2의 정보통신망을 통하여 유통되는 정보 중 인공지능 기술을 이용하여 만든 거짓의 음향·화상 또는 영상 등의 정보를 식별하고 하는 이를 인증하는 기관을 설립하는 근거규정은, 제52조의 형식을 따라 아래와 같이 규정하면 될 것으로 보인다.

정보통신망 이용촉진 및 정보보호 등에 관한 법률

(신설예시) 제00조(인공지능 기술을 이용한 거짓 정보의 식별 및 인증 기관의 설립)

- ① 정부는 정보통신망을 통하여 유통되는 정보 중 인공지능 기술을 이용하여 만든 거짓의 음향·화상 또는 영상 등의 정보를 식별하고 하는 이를 인증하기 위하여 (기관명)

126) 추후 입법논의 과정에서 주체를 어디로 할지 검토하여야 한다.

127) 추후 입법논의 과정에서 제1항의 주체가 정해지면 그에 맞추어 정하면 될 것이다.

을 설립한다.

3. 딥페이크 식별 기술 및 재정 지원을 위한 근거규정 마련

가. 딥페이크 식별 기술 지원 현황

1) 국내의 경우

딥페이크 감별 또는 식별 기술은 데이터셋을 기반으로 한 인공지능 기술이다. 이는 필연적으로 데이터베이스가 기반이 된 기술인데, 이러한 기존 변조/합성 탐지 연구 레퍼런스 데이터는 주로 서양인 위주로 구성되어 있다. 이에 국내에 해당 기술을 그대로 도입하기 위해서는 국내 데이터를 확보한 식별 기술 발전이 필요하며, 국내 실정에 맞는 식별 기술 개발 지원의 필요성이 크다. 이를 위하여 DFDC 같은 경진대회의 개최 또는 AI 학습용 데이터셋의 구축 및 배포 등의 방안이 고려될 수 있다. 위 방안들은 현재 국내에서 아래와 같이 시도되고 있다.

가) 서울대학교 · 한국정보화진흥원의 딥페이크 탐지 AI 경진대회 개최

서울대학교의 인공지능 연구실과 머니브레인(ManiBrain)은 최근 딥페이크 탐지 AI 경진대회를 개최하였다. 위 경진대회는 2020. 10. 19. 대회를 시작하여 2020. 11. 30. 시상식까지 마무리하는 과정으로 대략 40일 정도의 일정을 가지고 있다.

위 사업은 인터넷진흥원(NIA) 인공지능 데이터 사업의 일환으로 개최되는 것으로 인공지능 영상합성과 딥페이크 분야에서 세계적인 선두기업인 머니브레인과 서울대학교의 인공지능 연구실(DSAIL)이 주최, 테이콘이 주관, 한국정보화진흥원이 후원했다¹²⁸⁾.

128) <https://www.aitimes.kr/news/articleView.html?idxno=18184>

본 대회는 "AI hub 데이터 구축사업"의 일환으로써 "딥페이크 변조 영상 탐지"를 목적으로 하고 있다. 기존 변조/합성 탐지 연구 레퍼런스 데이터가 서양인 위주로 구성되고, 적은 데이터 양을 가지며, 탐지 방해 요소를 고려하지 않고 제작된 점 등의 문제점 해결하는 데이터를 제안함으로써 "AI hub 데이터 구축사업" 홍보 및 데이터 사용 활성화를 목적으로 한 것이다¹²⁹⁾. 본 대회의 주제는 딥페이크 변조 영상 탐지 및 다양한 딥페이크 변조 영상 탐지 모델 발굴이며 데이터콘에서 안내한 양식에 맞추어 코드를 제출하는 방식으로 참여가 이루어졌다.

나) 과학기술정보통신부의 AI 학습용 데이터 구축 사업 확정

딥페이크 식별을 위한 AI 학습 데이터셋 구축 및 배포는 식별 기술 개발 지원에 주요한 요소로 작용한다.

과학기술정보통신부는 'AI 학습용 데이터 구축 사업' 20개를 확정했다. 그 중 하나로 '딥페이크 방지 영상 AI 데이터' 기술도 포함돼 있다. 해당 과제는 머니브레인이 추진할 계획이며, 해당 업체는 딥페이크 방지에 필요한 영상 데이터를 제공할 계획이다¹³⁰⁾.

<그림삽입을 위한 여백>

129) <https://dacon.io/competitions/official/235655/overview/>

130) <https://www.sciencetimes.co.kr/news/%EB%B8%94%EB%A1%9D%EC%B2%B4%EC%9D%B8%EC%9C%BC%EB%A1%9C-%EB%94%A5%ED%8E%98%EC%9D%B4%ED%81%AC-%EB%8C%80%EC%9D%91%ED%95%A0-%EC%88%98-%EC%9E%88%EC%96%B4/>

[그림 5-1] 과학기술정보통신부 2020년 AI 학습용 데이터 구축 과제 선정 결과

지정공모(10개)		자유공모(10개)	
과제명	수행기관	과제명	수행기관
1 대용량 동영상 콘텐츠 AI데이터	KDX	질병진단 이미지 AI데이터	국립암센터
2 자율주행드론 비행 영상 AI데이터	울산대학교 산학협력단	도로환경 파노라마 이미지 AI데이터	울포랜드
3 시각정보 기반 질의응답 AI데이터	유클리드소프트	피트니스 자세 이미지 AI데이터	슬릭코퍼레이션
4 수어 영상 AI데이터	테스트웍스	K-Fashion 이미지 AI데이터	오피니언라이브
5 한국인 대화음성 AI데이터	솔루게이트	한국인 재식별 이미지 AI데이터	한국과학기술연구원
6 딥페이크 방지영상 AI데이터	머니브레인	도로주행영상 AI데이터	티큐에스코리아
7 랜드마크 이미지 AI데이터	피씨엔	치매진단 뇌파영상 AI데이터	디노플러
8 사람 인체·자세 3D AI데이터	스위트케이	감성 대화 말동치 AI데이터	미디어젠
9 문서요약 텍스트 AI데이터	비블라이소프트	위성영상 객체판독 이미지 AI데이터	한국항공우주연구원
10 전문분야 한영 말동치 AI데이터	플리토	구강악 2D·3D 이미지 AI데이터	헬스허브

위 AI 학습용 데이터 구축 사업은 2019년에 비하여 예산과 과제가 2배 늘어나 20개 과제를 390억원 규모로 추진하였다¹³¹⁾. 2019년에는 2개의 과제를 클라우드소싱 방식으로 추진하였으며 2020년에는 모든 과제에 클라우드소싱 방식을 적용한다.

클라우드소싱 방식을 적용하는 경우 데이터 구축의 효율성이 증대될 뿐만 아니라 일자리 창출효과까지 발생시킬 수 있다. 실제 2019년 AI 학습용 데이터 구축 사업 분석 결과, 일반적 데이터 가공은 10억당 38.1명, 클라우드소싱 방식은 10억당 200명의 일자리 창출 효과가 발생했다¹³²⁾.

따라서 데이터셋을 수집 및 배포하는 업무를 딥페이크 전담부서가 식별 기술 개발 지원의 일환으로 직접 수행하거나 혹은 수행을 지원하는 경우, 클라우드소싱 방법을 권장한다면 작업 시간의 효율성 및 일자리 창출 효과를 누릴 수 있을 것으로 예상된다.

131) 2019년에는 10개의 과제, 190여억 원의 예산 규모로 진행되었다.

132) <https://m.etnews.com/20200621000057>

2) 해외의 경우

해외에서도 딥페이크 식별기술의 개발을 위하여 여러 가지 지원이 이루어지고 있는데, 그 중 대표적인 것이 마이크로소프트이다.

마이크로소프트는 딥페이크를 악용한 허위 사진 및 영상의 유포와 남용을 막기 위하여 "디펜딩 데모크라시 프로그램(Defending Democracy Program)"을 진행하고 있다. 이 프로그램의 일환으로 비디오 어센터케이터 기술 개발이 이루어졌으며, 현재 마이크로소프트는 디펜딩 데모크라시 프로그램(Defending Democracy Program)을 통해 개발된 식별 기술을 적용 및 발전시키고 있다.

사실상 딥페이크의 남용 문제는 기술 개발의 측면에서만 보더라도 여러 분야가 협업해서 처리해야 한다. 이러한 견지에서 마이크로소프트는 식별 기술의 지속적 발전을 위한 적절한 협업체계를 구축한 것으로 보인다.

우선, 마이크로소프트는 AI 재단과 협업하여 AI 재단이 Reality Defender 2020(RD2020)을 통해 뉴스 매체 및 정치 캠페인을 포함하여 민주적 절차에 관련된 조직이 비디오 어센터케이터를 이용할 수 있도록 할 예정이다.

이에 더하여 마이크로소프트는 CNN을 포함한 여러 주요 언론 매체와 협업하여 비디오 어센터케이터의 기술을 광범위하게 적용하고 발전시킬 예정이다. 이러한 과정을 통하여 언론 매체에서도 위 식별 기술을 사용해 허위 영상 등을 분별하고 보다 정확한 정보를 전달할 수 있도록 할 것이며 이러한 작업을 통하여 위 식별 기술을 뉴스 및 소셜미디어(SNS)까지 확대하여 적용할 계획이다¹³³⁾.

3) 소결

국내에서는 서울대학교, 한국정보화진흥원, 과학기술정보통신부 등에 의하여 딥페이크 식별을 위한 AI 데이터 구축 지원이 이루어진바 있다. 아직 활발한 단계는 아니나

133) <https://blogs.microsoft.com/on-the-issues/2020/09/01/disinformation-deepfakes-newsguard-video-authenticator/>

그래도 이미 지원이 시작되었다는 점에 의의가 있다.

그러나 아직 국내 민간주도로는 딥페이크 식별 기술에 대한 지원이 활발하게 이루어지지 않고 있다. 마이크로소프트의 경우 적극적으로 딥페이크 식별을 위한 데이터셋 구축에 나서고 있는바, 위 사례를 참고하여 딥페이크의 악용 방지를 위한 기술의 지속적 개발 및 적용 분야 확대를 위하여 언론, 민간 재단 등과의 협업을 위한 프로그램을 출범하는 것도 식별 기술의 지속가능한 발전을 위한 방법 중 하나가 될 수 있다. 또한 아래와 같이 정부 차원에서 민간에 대한 딥페이크 식별 기술 지원을 위한 근거규정을 마련하는 것 또한 검토되어야 한다.

나. 딥페이크 식별 기술 지원 방안

딥페이크 식별을 위한 기술의 개발이 장려되어 식별 기술의 보급이 가능한 경우, 개발된 딥페이크 식별 도구는 공익 목적을 함유한다고 볼 수 있으므로 특정 도구들은 정부 주도하에 전담기관 또는 전담부서를 통하여 배포되는 것이 바람직하다.

현재 일부 악성코드 백신은 한국인터넷진흥원에 의하여 '보호나라' 홈페이지를 통해 배포되고 있다.¹³⁴⁾ 한국인터넷진흥원에서 위와 같은 백신배포를 담당하는 부서는 침해사고탐지팀이며 방송통신위원회의 구 네트워크정보보호팀은 인터넷진흥원과 협업하여 백신프로그램이용자안내서를 작성·배포하기도 하였다.

딥페이크 식별 도구를 배포하게 된다면 마찬가지로 위 보호나라 홈페이지가 활용될 수 있을 것으로 보인다. 딥페이크 식별 도구와 함께 딥페이크 식별 도구의 올바른 사용 방법 및 이용 수칙을 포함한 안내서를 함께 배포한다면 식별 도구의 활용도를 제고할 수 있을 것이다.

한편, 정부주도가 아닌 민간주도에 의하여 딥페이크 식별 기술의 개발을 장려하는 방안을 고려해볼 수 있다. 이를 위해 식별 도구 개발 및 배포에 대한 재정적 예산 지원, 경제적 유인 제공 등이 있을 수 있다.

134) https://www.boho.or.kr/download/dedicatedVaccine/downloadView.do?bulletin_writing_sequence=26603

또한 민간이 개발 및 배포하는 프로그램의 성능을 일정 수준 이상으로 담보하고 민간 개발 및 배포로 인한 부작용을 방지하기 위하여, 사업자를 위한 안내서를 발간하는 방법 역시 고려될 수 있다.

방송통신위원회와 한국인터넷진흥원은 앞서 언급한 이용자를 위한 백신 프로그램 이용 안내서 외에 사업자를 위한 올바른 백신 프로그램 안내서도 발간하여 불량 백신 프로그램의 배포를 방지한 바 있다¹³⁵⁾. 위 안내서는 사업자로 하여금 백신 프로그램 배포 시 준수해야 할 사항을 이행하도록 하여 불량 백신으로 인한 이용자의 피해를 최소화하고자 발간되었다¹³⁶⁾. 위 안내서는 백신 프로그램이 갖추어야 하는 주요 기능, 백신 배포시 고지해야 하는 사실과 동의를 받아야 하는 부분, 설명해야 하는 사항 등을 설명하여 백신 프로그램이 갖추어야 하는 기술 수준을 제시하고 배포 과정에서 발생하는 부작용을 최소화할 수 있도록 사업자에게 가이드라인을 제시하고 있다.

따라서 딥페이크 전담기관 또는 전담부서가 한국인터넷진흥원과 협업하여 민간이 배포하는 딥페이크 식별 프로그램에 대하여 사업자가 준수해야 하는 사항을 위와 같은 가이드라인 형식으로 제공한다면 사업자 및 이용자 모두를 지원할 수 있는 방안이 될 것이다.

다. 딥페이크 식별 기술 지원 근거규정 마련

딥페이크 식별 기술의 개발을 위하여는 정부가 주도하여 기술을 개발하여 보급하는 방안, 딥페이크 식별 기술 개발에 대한 재정적 지원 등을 통하여 민간주도에 의해 딥페이크 식별 기술을 개발 및 보급하는 방안이 있을 수 있다.

정보통신망법 제11조 제1항은 정부가 국가기관, 지방자치단체, 공공기관이 정보통신망 응용서비스를 개발, 운영하는 경우 그 기관에 재정 및 기술 지원을 할 수 있다고 되어야 있으며, 제11조 제2항 제5호는 정부가 민간부분에 의한 정보통신망 응용서비

135) https://www.boho.or.kr/data/guideView.do?bulletin_writing_sequence=1885

136) 방송통신위원회, 한국인터넷진흥원 「사업자를 위한 올바른 백신 프로그램 배포 가이드」, 2013. 2

스의 개발을 촉진하기 위하여 재정 및 기술 등 필요한 지원을 할 수 있고, 정보통신망 이용 교육프로그램의 개발 및 보급 지원을 위한 시책을 마련하여야 한다고 규정하고 있다. 동법 제41조 제1항 제1호에서는 방송통신위원회가 청소년유해정보로부터 청소년을 보호하기 위하여 내용 선별 소프트웨어의 개발 및 보급을 위한 시책을 마련하여야 한다고 규정하고 있으며, 제2항에서는 방송통신위원회가 제1항에 따른 시책을 추진할 때 정보통신서비스 제공자단체, 이용자단체, 그 밖의 관련 전문기관이 실시하는 청소년 보호를 위한 활동을 지원할 수 있다고 규정하고 있다. 동법 제50조의6 제1항은 방송통신위원회가 영리목적의 광고성 정보를 편리하게 차단하거나 신고할 수 있는 소프트웨어나 컴퓨터 프로그램을 개발하여 보급할 수 있다고 규정하면서, 제2항에서 방송통신위원회가 제1항에 따른 전송차단, 신고 소프트웨어 또는 컴퓨터 프로그램의 개발과 보급을 촉진하기 위하여 관련 공공기관, 법인, 단체 등에 필요한 지원을 할 수 있다고 규정하고 있다.

정보통신망 이용촉진 및 정보보호 등에 관한 법률

제11조(정보통신망 응용서비스의 개발 촉진 등)

① 정부는 국가기관·지방자치단체 및 공공기관이 정보통신망을 활용하여 업무를 효율화·자동화·고도화하는 응용서비스(이하 “정보통신망 응용서비스”라 한다)를 개발·운영하는 경우 그 기관에 재정 및 기술 등 필요한 지원을 할 수 있다.

② 정부는 민간부문에 의한 정보통신망 응용서비스의 개발을 촉진하기 위하여 재정 및 기술 등 필요한 지원을 할 수 있으며, 정보통신망 응용서비스의 개발에 필요한 기술인력을 양성하기 위하여 다음 각 호의 시책을 마련하여야 한다.

1. 각급 학교나 그 밖의 교육기관에서 시행하는 인터넷 교육에 대한 지원
2. 국민에 대한 인터넷 교육의 확대
3. 정보통신망 기술인력 양성사업에 대한 지원
4. 정보통신망 전문기술인력 양성기관의 설립·지원
5. 정보통신망 이용 교육프로그램의 개발 및 보급 지원
6. 정보통신망 관련 기술자격제도의 정착 및 전문기술인력 수급 지원
7. 그 밖에 정보통신망 관련 기술인력의 양성에 필요한 사항

제41조(청소년 보호를 위한 시책의 마련 등)

① 방송통신위원회는 정보통신망을 통하여 유통되는 음란·폭력정보 등 청소년에게 해로운 정보(이하 “청소년유해정보”라 한다)로부터 청소년을 보호하기 위하여 다음 각

호의 시책을 마련하여야 한다.

1. 내용 선별 소프트웨어의 개발 및 보급

2. 청소년 보호를 위한 기술의 개발 및 보급

3. 청소년 보호를 위한 교육 및 홍보

4. 그 밖에 청소년 보호를 위하여 대통령령으로 정하는 사항

② 방송통신위원회는 제1항에 따른 시책을 추진할 때에는 「방송통신위원회의 설치 및 운영에 관한 법률」 제18조에 따른 방송통신심의위원회(이하 “심의위원회”라 한다), 정보통신서비스 제공자단체·이용자단체, 그 밖의 관련 전문기관이 실시하는 청소년 보호를 위한 활동을 지원할 수 있다.

제50조의6(영리목적의 광고성 정보 전송차단 소프트웨어의 보급 등)

① 방송통신위원회는 수신자가 제50조를 위반하여 전송되는 영리목적의 광고성 정보를 편리하게 차단하거나 신고할 수 있는 소프트웨어나 컴퓨터프로그램을 개발하여 보급할 수 있다.

② 방송통신위원회는 제1항에 따른 전송차단, 신고 소프트웨어 또는 컴퓨터프로그램의 개발과 보급을 촉진하기 위하여 관련 공공기관·법인·단체 등에 필요한 지원을 할 수 있다.

③ 방송통신위원회는 정보통신서비스 제공자의 전기통신역무가 제50조를 위반하여 발송되는 영리목적의 광고성 정보 전송에 이용되면 수신자 보호를 위하여 기술개발·교육·홍보 등 필요한 조치를 할 것을 정보통신서비스 제공자에게 권고할 수 있다.

④ 제1항에 따른 개발·보급의 방법과 제2항에 따른 지원에 필요한 사항은 대통령령으로 정한다.

위와 같이 기존 정보통신방법에는 특정 소프트웨어의 개발 및 보급에 관한 규정을 두고 있는바, 딥페이크 식별 기술의 개발 및 보급을 위한 근거마련 또한 정보통신망법 제11조 제1,2항, 제41조 제1,2항, 제50조의6 제1,2항 등을 참조하여 아래와 같이 규정할 수 있을 것이다.

정보통신망 이용촉진 및 정보보호 등에 관한 법률

(신설예시) 제00조(인공지능 기술을 이용한 거짓정보 식별 소프트웨어의 보급 등)

① 방송통신위원회는 정보통신망을 통하여 유통되는 정보 중 인공지능 기술을 이용하여 만든 거짓의 음향·화상 또는 영상 등의 정보를 식별하는 소프트웨어나 컴퓨터프로그램을 개발하여 보급할 수 있다.

② 방송통신위원회는 제1항에 따른 소프트웨어 또는 컴퓨터프로그램의 개발과 보급을 촉진하기 위하여 관련 공공기관·법인·단체 등에 필요한 지원을 할 수 있다.

③ 제1항에 따른 개발·보급의 방법과 제2항에 따른 지원에 필요한 사항은 대통령령으로 정한다.

이외에도 정보통신망법은 동법 제4조 제2항 시책과 관련하여 여러 규정을 두고 있는바, 그 중에 관련기관에 대한 재정 및 기술 지원에 대한 내용을 담고 있는 조항이 있어 이를 참고할만하다.

구체적으로, 정보통신망법 제6조 제1항은 과학기술정보통신부장관은 정보통신망과 관련된 기술 및 기기의 개발을 효율적으로 추진하기 위하여 대통령령으로 정하는 바에 따라 관련 '연구기관'으로 하여금 연구개발 등의 사업을 하게 할 수 있다고 규정하고 있으며, 제6조 제2항은 정부가 위 연구기관에 '사업비용의 전부 또는 일부를 지원'할 수 있다고 규정하고 있다. 동법 제11조 제1항에서는 정부가 국가기관, 지방자치단체 및 공공기관이 정보통신망을 활용하여 업무를 효율화, 자동화, 고도화하는 응용서비스를 개발, 운영하는 경우 그 '기관'에 '재정 및 기술 등 필요한 지원'을 할 수 있다고 규정하고 있으며, 동조 제2항에서는 정부가 정보통신망 '전문기술인력 양성기관의 설립, 지원'에 관한 시책을 마련하여야 한다고 규정하고 있다. 동법 제12조 제2항에서는 정부가 동조 제1항에 따른 정보의 공동활용체제를 구축하는 자에게 '재정 및 기술 등 필요한 지원'을 할 수 있다고 규정하고 있다. 동법 제10조에서는 정부는 국가경쟁력을 확보하거나 공익을 증진하기 위하여 정보통신망을 통하여 유통되는 정보내용물을 개발하는 자에게 '재정 및 기술 등 필요한 지원'을 할 수 있다고 규정하고 있다.

<표 4-4> 정보통신망법 상 기관에 대한 기술 및 재정 지원 관련 규정

정보통신망법 제4조 제2항 시책	관 련 조 항
1. 정보통신망에 관련된 기술의 개발·보급	제6조(기술개발의 추진 등) ① 과학기술정보통신부장관은 정보통신망과 관련된 기술 및 기기의 개발을 효율적으로 추진하기 위하여 대통령령으로 정하는 바에 따라 관련 <u>연구기관으로 하여금 연구개발·기술협력·기</u>

	<u>술이전 또는 기술지도 등의 사업을 하게 할 수 있다.</u> ② 정부는 제1항에 따라 연구개발 등의 사업을 하는 <u>연구기관에는 그 사업에 드는 비용의 전부 또는 일부를 지원할 수 있다.</u> ③ 제2항에 따른 비용의 지급 및 관리 등에 필요한 사항은 대통령령으로 정한다.
3. 정보내용물 및 제11조에 따른 정보통신망 응용서비스의 개발 등 정보통신망의 이용 활성화	제11조(정보통신망 응용서비스의 개발 촉진 등) ① 정부는 국가기관·지방자치단체 및 공공기관이 정보통신망을 활용하여 업무를 효율화·자동화·고도화하는 응용서비스(이하 “정보통신망 응용서비스”라 한다)를 개발·운영하는 경우 <u>그 기관에 재정 및 기술 등 필요한 지원을 할 수 있다.</u>
4. 정보통신망을 이용한 정보의 공동활용 촉진	제12조(정보의 공동활용체제 구축) ① 정부는 정보통신망을 효율적으로 활용하기 위하여 정보통신망 상호 간의 연계 운영 및 표준화 등 정보의 공동활용체제 구축을 권장할 수 있다. ② 정부는 제1항에 따른 <u>정보의 공동활용체제를 구축하는 자에게 재정 및 기술 등 필요한 지원을 할 수 있다.</u> ③ 제1항과 제2항에 따른 권장 및 지원에 필요한 사항은 대통령령으로 정한다.
7의2. 정보통신망을 통하여 유통되는 정보 중 인공지능 기술을 이용하여 만든 거짓의 음향·화상 또는 영상 등의 정보를 식별하는 기술의 개발·보급	관련 규정 없음
9. 그 밖에 정보통신망 이용촉진 및 정보보호등을 위하여 필요한 사항	제10조(정보내용물의 개발 지원) 정부는 국가경쟁력을 확보하거나 공익을 증진하기 위하여 정보통신망을 통하여 유통되는 <u>정보내용물을 개발하는 자에게 재정 및 기술 등 필요한 지원을 할 수 있다.</u>

위와 같이 기존 정보통신망법에는 정부가 특정 기술을 개발하는 기관에 재정 및 기술 등 필요한 지원을 할 수 있다는 규정을 두고 있는바, 딥페이크 식별 기술을 개발

하는 기관에 대한 지원에 대하여도 아래와 같이 규정할 수 있을 것이다.

정보통신망 이용촉진 및 정보보호 등에 관한 법률

(신설예시) 제00조(인공지능 기술을 이용한 거짓정보 식별기술의 개발 지원)

(정부/방송통신위원회)는 정보통신망을 통하여 유통되는 정보 중 인공지능 기술을 이용하여 만든 거짓의 음향·화상 또는 영상 등의 정보를 식별하는 기술을 개발하는 기관에 재정 및 기술 등 필요한 지원을 할 수 있다.

4. 결어

이상에서 딥페이크 식별 및 인증을 위한 기관 지정 또는 설립, 그 근거규정 마련, 딥페이크 식별 기술 지원 방안, 기술 등 지원을 위한 근거규정 마련 등에 관하여 살펴보았다.

위에서 살펴본 바와 같이, 최근 개정된 정보통신망법 제4조 제2항 제7의2호는 딥페이크 식별 기술의 개발·보급을 위한 시책마련을 규정하고 있으나, 아직까지 구체적인 시책이 마련되어 있지 아니하다. 국내에서는 해외와는 달리 민간주도에 의하여 딥페이크 식별 기술에 대한 지원이 적극적으로 이루어지지 않고 있으며, 서울대학교, 한국정보화진흥원, 과학기술정보통신부 등 소수의 기관에 의하여 딥페이크 식별을 위한 AI 데이터 구축 지원이 이루어진 것에 그치고 있다.

한편, 2019년 방송통신발전 기본법 일부개정 법률안에서 딥페이크 식별 및 인증을 위한 전담기구의 운영을 위한 기금사용을 다룬 적이 있으나, 위 법안은 임기만료로 폐기되었으며, 이후 동일한 취지의 논의가 이루어지지 않고 있다. 현재 딥페이크의 부작용을 방지하고 해소하기 위한 별다른 제도가 추진되고 있지 아니한바, 현재와 같은 상황에서는 식별 및 인증을 위한 전담기구의 운영에 관한 논의도 진척되기 어려운 상황이다. 그러나 딥페이크 식별 및 인증 전담기구의 운영에 관하여 지속적인 논의가 필요하다.

나아가 딥페이크 식별을 위한 기술의 개발이 장려되어 식별 기술의 보급이 가능한 경우, 이는 일차적으로 정부 주도하에 전담기관 또는 전담부서를 통하여 배포되는 것이 바람직하나, 식별 도구 개발 및 배포에 대한 재정적 예산 지원, 경제적 유인 제공 등을 제공하여 민간을 통한 개발 및 배포를 장려할 수도 있을 것이다.

제6절 딥페이크 관련 범부처협의체 등의 운영

1. 서설

위에서 살펴본 바와 같이 딥페이크 기술은 여러 법령 및 제도와 연관되어 있다. 이에 딥페이크 기술을 본격적으로 다룰 기관 또는 부처를 어디로 하여야 할지, 범부처 협의체를 설립하여야 할지에 대한 논의가 필요하다.

범부처 협의체는 여러 부처의 협업을 위하여 만들어지는 특정 기술 등에 있어 여러 부처를 총괄하는 기관이자 최종의사결정을 내리는 기관이다. 전담부서는 여러 부처를 총괄하지는 아니하나 특정 기술 등에 관한 전반적인 총괄 및 최종의사결정을 내리고 타 부서의 협업이 필요한 경우 이를 요청하여 진행할 수 있다.

딥페이크는 앞서 살펴본 바와 같이 기술의 적용 범용성이 높아 음란물, 명예훼손 등의 범죄물, 선거 홍보물 혹은 비방물, 그리고 그 외 AI에의 적용 등 다양한 방면에서 활용 및 악용될 수 있다.

이렇듯 딥페이크 기술은 다양한 분야에서 활용되는 방면 이를 규제하는 전담부서 또는 범부처협의체가 부재한바, 딥페이크 기술을 악용하여 문제가 발생하더라도 효율적이고 신속한 대처가 이루어지기 어려운 실정이다. 또한 딥페이크의 활용 실태 등에 관한 총체적인 조사, 모니터링도 이루어질 수 없다. 실태조사 또는 모니터링이 없다면 실제 지원이 필요한 부분을 확정하는 것이 어렵다.

딥페이크를 효과적으로 규율하기 위해서는 현재 딥페이크가 어떤 분야에서 어떤 방식으로 사용되고 있으며 악용 현황은 어떠한지에 관한 파악이 우선적으로 이루어져야 하고, 이후 조사된 내용에 기반하여 식별 기술 등을 개발하고 여러 분야에 적용·배포하는 과정이 필요하다. 위 과정은 서로 유기적으로 연결되어 있으므로 일련의 과정을 총괄할 수 있는 범부처협의체 또는 전담부서 등의 운영이 필수적이다.

이하에서는 딥페이크와 관련된 범부처협의체 또는 전담부서의 운영에 관하여 검토 하도록 한다.

2. 딥페이크 관련 전담부서의 운영

가. 딥페이크 관련 전담부서의 업무

딥페이크와 관련한 전담 부서는 딥페이크 활용/악용 실태 파악, 모니터링, 워터마크 표시의무제도 등 관련 제도관리, 유통규제, 식별 기술, 보급을 위한 시책마련, 관련 법안 발의 및 법률제개정, 기술 배포 및 상용화 지원, 보고서 작성 등을 주로 담당하게 될 것이다.

현재 딥페이크 기술 관련 업무에 관하여 다루고 있는 법령은 정보통신망법이 유일하며, 정보통신망법 제4조 제1항, 제2항 제7의2호에서는 과학기술정보통신부장관 또는 방송통신위원회로 하여금 정보통신망을 통하여 유통되는 정보 중 인공지능 기술을 이용하여 만든 거짓의 음향·화상 또는 영상 등의 정보를 식별하는 기술의 개발·보급에 관한 시책을 마련할 것을 규정하고 있다. 현재 정보통신망법 상 식별 기술의 개발과 보급에 한정되어 시책마련 의무가 있으나, 아직 구체적인 시책이 나와 있는 것은 없다.

정보통신망 이용촉진 및 정보보호 등에 관한 법률

제4조(정보통신망 이용촉진 및 정보보호등에 관한 시책의 마련)

① 과학기술정보통신부장관 또는 방송통신위원회는 정보통신망의 이용촉진 및 안정적 관리·운영과 이용자 보호 등(이하 "정보통신망 이용촉진 및 정보보호등"이라 한다)을 통하여 정보사회의 기반을 조성하기 위한 시책을 마련하여야 한다.

② 제1항에 따른 시책에는 다음 각 호의 사항이 포함되어야 한다.

7의2. 정보통신망을 통하여 유통되는 정보 중 인공지능 기술을 이용하여 만든 거짓의 음향·화상 또는 영상 등의 정보를 식별하는 기술의 개발·보급

한편 2019년 이종걸의원은, 딥페이크 합성 영상의 무분별한 유통으로 인한 피해를 예방하기 위하여 방송통신위원회가 합성 영상으로 인한 명예훼손 등의 피해 실태 파악, 합성 영상 유통 실태 및 관련 국내외 기술 동향 파악, 유통 방지를 위한 기술 개발의 촉진, 교육·홍보 등의 시책을 추진하도록 함으로써 건전한 정보통신망 이용환경을 조성하려는 목적으로 정보통신망법 제44조의9(합성 영상으로 인한 피해예방을 위한 시책)의 신설을 제안한바 있고, 해당 신설안(의안번호 2024319)은 방송통신위원회로 하여금 ① 합성 영상으로 인한 명예훼손 등의 피해 실태 파악, ② 합성 영상 유통 실태 파악, ③ 합성 영상 관련 국내외 기술동향 파악, ④ 합성 영상의 무분별한 유통 방지를 위한 기술 개발의 촉진, ⑤ 합성 영상의 무분별한 유통 방지 및 피해 예방을 위한 교육·홍보, ⑥ 그 밖에 합성 영상의 무분별한 유통 방지 및 피해 예방에 필요한 사항에 관한 시책을 추진하여야 한다고 규정하고 있었다.

정보통신망 이용촉진 및 정보보호 등에 관한 법률

제44조의9(합성 영상으로 인한 피해예방을 위한 시책) 방송통신위원회는 사람을 대상으로 한 영상에 다른 사람의 얼굴이나 신체 부위의 이미지를 중첩하거나 결합하여 만든 합성 영상의 무분별한 유통으로 인한 피해를 예방하기 위하여 다음 각 호의 시책을 추진하여야 한다.

1. 합성 영상으로 인한 명예훼손 등의 피해 실태 파악
2. 합성 영상 유통 실태 파악
3. 합성 영상 관련 국내외 기술동향 파악
4. 합성 영상의 무분별한 유통 방지를 위한 기술 개발의 촉진
5. 합성 영상의 무분별한 유통 방지 및 피해 예방을 위한 교육·홍보
6. 그 밖에 합성 영상의 무분별한 유통 방지 및 피해 예방에 필요한 사항

위 신설안은 국회임기만료로 폐기되었으며, 정보통신망법 제4조 제1항, 제2항 제7의2호가 도입되면서, 추가적으로 동일한 취지의 신설안의 제안되거나 하지는 않은 상황이다.

비록 폐기되기는 하였으나 위 신설안이 딥페이크 영상에 대한 시책을 구체적으로 나열한 것은 참조할만한 하다. 정보통신망법 제4조 제1항, 제2항 제7의2호는 딥페이크

를 식별하는 기술의 개발·보급에 관한 시책을 마련할 것만을 규정하고 있으나, 위 신설안은 딥페이크 관련 실태파악, 기술동향 파악, 딥페이크 영상의 유통규제, 피해예방 까지 시책의 범위를 다양하게 규정하였다.

참고로 미국의 Accoutability Act¹³⁷⁾는 국토안보부 장관에게 다른 관련 연방기관의 수장과 협력하여, 과학기술국(Science and Technology Directorate) 내에 'Deep Fakes Task Force'를 설립하도록 의무를 부여하고 있는바(SEC. 7 (a)), 미국의 'Deep Fakes Task Force'는 딥페이크 등 발전된 이미지 조작 방법을 감지, 방지, 딥페이크 등 위조된 것과 합법적인 시청각 자료들을 구별하기 위한 기술을 연구·개발하고((2)), 그러한 기술을 연구하는 다른 연방기관에 행정적, 과학적 지원을 제공하기 위하여 설립되었다((3)). 미국은 위 TF를 통하여 식별에 관한 기술 개발 지원 및 연구를 직접 수행하고 딥페이크 식별을 위한 통합적 기술 개발을 Task Force의 책임 하에 진행하도록 하고 있다. 또한 TF의 역할은 대부분 딥페이크 관련 기술 개발과 연관되어 있어, 딥페이크 전담부서의 업무는 딥페이크와 관련한 실태 조사, 기술 현황 파악, 그리고 기술 개발 지원에 집중되어 있다.

이렇듯 딥페이크 관련 전담부서가 지정되는 경우 해당 부서의 업무는 딥페이크 관련 실태파악, 식별 기술의 개발·보급 지원, 딥페이크 영상의 유통규제, 피해예방 등이 될 것이다.

나. 음란물 및 선거물 관련

1) 음란물 관련

딥페이크가 가장 많이 악용되는 분야 중 하나는 음란물이다. 현행 성폭력처벌법은 딥페이크라는 단어를 사용하지는 않지만 “반포 등을 할 목적으로 사람의 얼굴·신체 또는 음성을 대상으로 한 촬영물·영상물 또는 음성물을 대상자의 의사에 반하여 성적

137) 아직 시행되지 아니하였다.

욕망 또는 수치심을 유발할 수 있는 형태로 편집·합성 또는 가공한 자”는 5년 이하의 징역 또는 5천만원 이하의 벌금에 처하며, 이러한 편집물 등을 반포한 자도 동일한 수준으로 처벌하고 있다(성폭력처벌법 제14조의2).

이처럼 딥페이크를 활용한 음란영상물에 대해 성폭력처벌법에서 다루고 있는바, 딥페이크를 활용한 음란물에 관한 업무는 디지털 성범죄에 관한 전담부서가 맡아 딥페이크 피해자 지원, 수사 지원, 그리고 디지털 자료 삭제 피해자 지원 등을 행하는 것이 효율적일 것이다.

현재 디지털 성범죄에 관하여 위 각 지원을 행하는 전담부서는 각 지방자치단체별로 신설되어 운영되고 있다. 서울특별시는 지원이 가장 필요한 아동·청소년 피해자를 위주로 하는 디지털 성범죄 전담 Task Force를 추진 중이며, 경기도 역시 디지털 성범죄 피해자 지원 전담 조직을 설치하였다. 경기도의 전담 조직은 특정 음란물을 찾아내 방송통신심의위원회를 통해 해당 기록이 인터넷에서 삭제될 수 있도록 하고 피해자들을 수사기관 등 관련 기관과 연계해 지원하는 형태로 운영되며, 디지털 성범죄 대응 감시단을 신설하여 딥페이크 등 불법 게시물을 탐지하는 역할도 수행 중이다.

한편, 방송통신심의위원회는 디지털성범죄심의회지원단의 24시간 상황실 운영, 전담 소위원회 신설, 전자심의시스템 도입을 통해 디지털성범죄에 대응하고 있으므로, 디지털 성범죄 전담부서와 협력하여 음란물 대응이 가능하다.

2) 선거 관련

딥페이크는 선거 관련 홍보물 혹은 비방을 위한 목적으로도 사용될 수 있다. 선거와 관련하여 딥페이크 기술을 사용하는 것은 주로 허위의 사실을 유포하기 위함인바, 이는 공정선거를 방해하고 선거법에 위반하는 행위가 될 수 있다.

중앙선거관리위원회는 선거법 위반행위 및 공정선거를 위한 사항을 총괄하고 있으며, 선거법 위반사항에 관하여는 신고를 받고, 위반 혐의에 관하여 검찰에 고발 및 수사를 의뢰한다.

특히 사이버상 선거법 위반행위에 대한 감시 및 단속을 위한 별도 사이버공정선거지원단이 운영되고 있는바 딥페이크가 선거법 위반 행위로 규명되거나 선거법 위반의 소지가 있는 종류의 게시글로 발현되는 경우에는 사이버공정선거지원단을 활용하여 관리가 가능할 것으로 보인다.

한편, 현행 공직선거법 제82조의4 제3항에 따르면, 선거관리위원회 또는 후보자(후보자가 되고자 하는 자 포함)는 공직선거법에 위반되는 정보가 인터넷 홈페이지 또는 그 게시판대화방 등에 게시되거나, 정보통신망을 통하여 전송되는 사실을 발견할 때에 인터넷홈페이지 관리·운영자에게 해당 정보의 삭제를 요청하거나, 인터넷홈페이지 관리·운영자 또는 정보통신서비스제공자에게 그 취급의 거부·정지·제한을 요청할 수 있는데, 방송통신심의위원회가 보유하고 있는 정보통신 분야에 대한 모니터링 및 심의 전문성에도 불구하고, 유독 선거 관련 불법정보에 관하여는 방송통신심의위원회의 모니터링, 심의 권한이 배제되어 있다. 이는 공직선거법에서 선거기간 중 방송통신심의위원회로 하여금 한시적으로 선거방송심의위원회¹³⁸⁾라는 임시기구를 운영하도록 한 것과 대비된다.

선거방송심의와의 균형을 고려하고 통신심의 및 불법정보 모니터링에 대한 방송통신심의위원회의 전문 역량을 활용하여 유권자의 진정한 의사 왜곡을 방지하는 취지로, 선거기간 중 한시적으로 선거방송심의위원회에 준하는 임시기구를 운영하는 방안을 진지하게 고려할 필요가 있다.

3. 딥페이크 관련 범부처협의체 운영

138) 공직선거법

제8조의2(선거방송심의위원회) ① 「방송통신위원회의 설치 및 운영에 관한 법률」 제18조제1항에 따른 방송통신심의위원회(이하 "방송통신심의위원회"라 한다)는 선거방송의 공정성을 유지하기 위하여 다음 각 호의 구분에 따른 기간 동안 선거방송심의위원회를 설치·운영하여야 한다.

범부처협의체는 특정한 목적을 달성하기 위하여 각 부서 간 산재된 정책의 통일성을 기하고, 부처 간 협업을 통해 보다 효율적인 정책을 연구 및 추진하기 위하여 구성되는 것으로서, 여러 부처를 총괄하는 기관이자 최종의사결정을 내리는 기관이다.

범부처협의체는 청와대 관련보좌관, 국무조정실 등이 주재하여 부처간의 협업이 필요한 분야에서 대책을 마련하고 시행하기 위하여 진행되거나, 특정한 연구 등의 목적을 위하여 법률이 사업의 공동운영규정을 마련하고 있는 경우에 진행된다. 일례로 국무조정실 교육문화여성정책관실은 디지털 성범죄 대응을 위하여 디지털 성범죄에 관한 다차원적인 피해자 구제 및 처벌 강화 등을 위하여 구성되었으며, 법무부, 방송통신위원회, 여성가족부, 과학기술정보통신부 등을 포함한 디지털 성범죄 근절대책 회의를 주재하였으며 디지털 성범죄 근절을 위한 각 부처의 협업을 유도하였다. 또한 과학기술정보통신부훈령인 포스트게놈 다부처유전체사업 공동운영규정에 의하여 보건복지부, 과학기술정보통신부, 산업통상자원부 등의 부처간 범부처협의체를 구성하여 포스트게놈에 관하여 논의가 이루어졌다.

현재 딥페이크 관련 사안에 대한 범부처협의체 구성 근거 규정이 없는 상황이므로, 딥페이크 관련 범부처협의체는 청와대 관련 보좌관, 국무조정실 등의 판단 아래 구성될 수 있을 것으로 보인다.

위에서 딥페이크와 관련된 현안에 관하여 살펴보았는바, 딥페이크 기술에 관한 각 부서 간 추진업무의 통일성을 기하고, 부처 간 협업을 통해 효율적인 정책을 연구 및 추진하기 위하여 방송통신위원회, 과학기술정보통신부, 법무부, 경찰청 등으로 구성된 딥페이크 기술 관련 범부처 협의체의 구성을 고려해볼 수 있다.

4. 결어

위에서 살펴본 바와 같이, 딥페이크와 관련한 전담 부서는 딥페이크 활용/악용 실태 파악, 모니터링, 워터마크 표시의무제도 등 관련 제도관리, 유통규제, 식별 기술 개발 및 보급 관련 시책 마련, 관련 법안 발의 및 법률제개정, 기술 배포 및 상용화 지

원, 보고서 작성 등을 주로 담당하게 될 것으로 보이며, 앞으로 딥페이크 관련 업무가 더욱 구체적으로 대두되는 경우 전담부서의 지정이 필요할 수 있다.

나아가 딥페이크 기술을 이용한 음란물의 경우 기존에 디지털 성범죄 업무를 담당 하던 각 지방자치단체별 디지털 성범죄 피해자 지원 전담 조직을 활용할 수 있을 것이며, 방송통신심의위원회의 디지털성범죄심의회지원단과도 협력이 가능하다. 딥페이크 기술을 활용한 선거물의 경우 중앙선거관리위원회, 사이버공정선거지원단 등에서 업무를 담당할 수 있을 것으로 보인다.

또한 딥페이크 기술은 여러 법령 및 제도와 연관되어 있고 기술의 범용성이 넓은 특성으로 인하여 각 부처 별로 관련 업무가 산재되어 있다. 이에 딥페이크 관련 정책의 통일성을 기하고, 효율적인 정책 및 연구를 추진하기 위하여 방송통신위원회, 과학기술정보통신부, 법무부, 경찰청, 여성가족부, 선거관리위원회 등으로 구성된 딥페이크 기술 관련 범부처 협의체의 구성을 고려해볼 수 있다.

제5장 결론

이상에서 딥페이크 기술과 관련된 기술동향 및 해외 입법 동향을 파악하고, 딥페이크 관련 국내 입법 및 제도 개선방안, 딥페이크 관련 규제체계 전반 등을 논의하기 위한 전담부서 및 범부처 협의체 구성 및 운영방안에 관하여 살펴보았다.

딥페이크 생성기술은 문화콘텐츠, 의료 등 분야에서 유용한 기술로서 사용되고 있지만, 음란물 등 디지털성범죄, 명예훼손, 선거범죄 등에 악용될 가능성이 크다. 딥페이크 생성기술은 이윤창출의 효과가 분명하기에 급속도로 발전 중이다. 그러나 딥페이크 식별 기술의 발전은 더딘 상황이다. 딥페이크 기술로 인한 부작용을 줄이고, 피해를 예방하기 위하여 국가적인 차원에서 딥페이크 식별 기술 발전을 지원해야 할 필요성이 있다.

해외에서는 이러한 딥페이크 기술에 대한 사회적 부작용을 줄이기 위하여 선제적으로 법률안을 마련하였으며, 그 중 몇몇 국가에서는 이미 관련 법이 시행중이다. 딥페이크에 관하여 가장 적극적으로 입법활동을 하고 있는 국가는 미국이며, 미국 연방차원에서 입법 추진되고 있는 법안이 상당히 구체적이나 아직 본격적으로 시행되지는 않고 있다. 미국은 연방차원의 법안 이외의 각 주에서도 딥페이크를 음란물, 프라이버시, 명예훼손, 개인정보, 플랫폼 사업자의 책임, 선거, 가짜뉴스 등 여러 주제에서 접근하여 법을 마련하거나 입법이 추진되고 있다. 그 이외의 국가들은 딥페이크에 대하여 정면으로 다룬 독립된 법안을 가지고 있지 아니하나, 온라인콘텐츠, 플랫폼사업자, 선거, 부정확한 정보의 유통 방지 등 특정 이슈에 맞게 입법이 추진되거나 관련 법이 시행되고 있다.

딥페이크 기술은 음란물, 명예훼손, 퍼블리시티권, 초상권 침해, 저작권, 보이스피싱, 피해자의 삭제, 처리정지 등 조치요구, 정보통신서비스 제공자의 의무와 책임, 선거 등 법적이슈와 관련되어 있는데, 현재 국내에서는 딥페이크 관련하여 단독으로 법률안이 발의한 된 것은 없으며, 최근 딥페이크 기술로 제작한 음란영상물을 규제하기

위한 성폭력처벌법 제14조의2가 신설된 것을 시작으로, 정보통신망법에 딥페이크와 관련된 여러 조항이 도입되어 시행되고 있다. 정보통신망법에서는 과학기술정보통신부장관 또는 방송통신위원회로 하여금 딥페이크 관련 기술에 관한 시책을 마련하도록 하였고(정보통신망법 제4조 제2항 7의2호), 일정규모 이상의 정보통신서비스 제공자로 하여금 딥페이크 기술로 생성된 음란물의 유통을 방지하기 위한 책임자를 지정하고(동법 제44조의 9), 불법촬영물 등의 유통방지와 관련된 각종 사항에 대한 보고서 작성 및 제출 의무를 부여하였다(동법 제64조의5).

딥페이크 관련 이슈는 기존 국내 법령으로도 상당부분 해결되고 있는 상황이어서 심각한 입법공백이 있지는 아니한 것으로 보인다. 다만 성폭력처벌법 제14조의2(허위영상물 등의 반포등) 제1항 상 목적조항의 삭제 또는 유지여부, 성폭력처벌법 제14조의2 내 소지행위 처벌규정 신설여부가 검토되어야 할 것으로 보이며, 해외에서 딥페이크 관련 논의가 선거법 쪽에서 활발하게 일어나고 있는 것에 비하여 국내에서는 아직까지 이렇다 할 개정작업이 진행되지 않고 있어, 해외 사례에 비추어 국내 공직선거법을 개선하여야 할지에 대한 추가적인 검토가 필요해 보인다.

이처럼 딥페이크 기술과 관련한 입법이 최근에서야 본격적으로 진행되고 있는 상황이며, 정보통신망법 상 딥페이크 식별 기술 개발, 보급 관련 시책마련 의무가 도입되어 있기는 하나, 아직 이렇다 할 구체적인 시책이 마련되지 않았고, 딥페이크 관련된 제도도 신설되지 않고 있다. 이에 앞으로 딥페이크 기술과 관련되어 어떤 제도를 시행하면 딥페이크로 인한 사회적인 부작용을 효과적으로 줄일 수 있을지, 그러한 제도의 도입을 위하여 입법적으로 어떻게 근거규정을 마련할지에 관하여 검토가 진행되었다.

딥페이크에 대한 사전규제책으로서의 유통 신고·허가제가 있을 수 있으나, 헌법상 사전검열에 해당하여 실제로 추진하기 쉽지 않다. 딥페이크에 관한 사후규제책으로 딥페이크 영상 생성 이후 유통시 워터마크 표시의무, 변경내용표시의무 제도를 도입하는 것을 검토해볼 수 있으며, 정보통신망법 상 근거규정을 마련하여 시행하면 될 것으로 보인다. 그 외 사후규제책으로서, 플랫폼 보류대기 시스템, 지정플랫폼의 운영

등을 검토해볼 수 있으나, 아직 딥페이크 식별 기술이 완전하지 못하고 대중적으로 보급되지 않은 점, 자칫하면 사전허가제로 변질되어 운영될 우려가 있다는 점 등 때문에 실제 시행은 쉽지 않아 보인다.

한편, 딥페이크 피해자의 구제강화 방안으로 딥페이크 피해자의 삭제요구권 강화, 국내대리인 지정제도의 활용을 고려해볼 수 있으며, 딥페이크 식별 기술의 발전을 위해 딥페이크 식별 및 인증을 위한 기관 지정 또는 설립, 정부 차원에서의 딥페이크 식별 기술에 대한 지원이 고려될 수 있다.

마지막으로 딥페이크 활용/악용 실태 파악, 모니터링, 워터마크 표시의무제도 등 관련 제도관리, 유통규제, 식별 기술, 보급을 위한 시책마련, 관련 법안 발의 및 법률제 개정, 기술 배포 및 상용화 지원, 보고서 작성 등 딥페이크 관련 여러 업무를 총괄적으로 처리하기 위한 전담부서의 지정을 고려해볼 수 있다.

나아가 딥페이크 기술에 관한 각 부서 간 추진업무의 통일성을 기하고, 부처 간 협업을 통해 효율적인 정책을 연구 및 추진하기 위하여 방송통신위원회, 과학기술정보통신부, 법무부, 경찰청 등으로 구성된 딥페이크 기술 관련 범부처협의체의 구성이 요구되는 바이다.

위에서 언급한 내용을 최종적으로 정리하면 아래와 같다.

<표 6-1> 딥페이크 기술 관련 입법 및 제도 개선 논의

	이슈	관련법령	개선논의
국내 입법 현황 및 개선 논의	음란물	성폭력처벌법 제14조의2(허위영상물 등의 반포등), 제15조(미수범)	○ (개선논의) 성폭력처벌법 제 14조의2 제1항 목적조항의 삭제 여부 ○ (규정신설검토) 소지 행위에 대한 처벌규정 검토
		정보통신망법 제44조의7(불법정보의 유통금지 등) 제1항 제1호, 제74조(벌칙)	

	제1항 제2호	
명예훼손 · 사자명예훼손	형법 제307조(명예훼손), 제309조(출판물등에 의한 명예훼손)	
	정보통신망법 제70조(벌칙), 제44조의7(불법정보의 유통금지 등)	
	형법 제308조(사자의 명예훼손)	
퍼블리시티권 · 초상권 침해	판례, 학설 등에 의하여 인정되는 권리	
저작권	저작권법 제136조 제1항 제1호	
보이스피싱	통신사기피해환급법 제15조의 2(벌칙)	
선거	공직선거법 제110조(후보자 등의 비방금지), 제250조(허위사실공표죄)	○ (개선논의) 해외에서는 선거 관련하여 딥페이크 영상에 관한 논의가 활발하며 선거일을 기준 으로 하여 구체적인 처벌규정을 마련하고 있는바, 현행 공직선거 법 상 개선점이 있는지 검토할 필요가 있음
피해자의 삭제 · 처리정지 등 조치요구	개인정보보호법 제36조(개인정보의 정정 · 삭제), 제37조(개인정보의 처리정지 등)	
	정보통신망법 제44조의2(정보의 삭제요청 등)	
	성폭력처벌법 일부개정법률안 제31조 제3항	

	플랫폼 운영자의 책임과 의무	정보통신망법 제44조(정보통신망에서의 권리보호)	
		정보통신망법 제44조의2(정보의 삭제요청 등), 제44조의3(임의의 임시조치)	
		정보통신망법 제44조의7(불법정보의 유통금지 등)	○ (입법공백) 정보통신망법 제 44조의7 제3항 제1호에 성폭력 처벌법 제14조의2 포함여부 검 토
		정보통신망법 제44조의9(불법촬영물등 유통방지 책임자), 제76조(과태료) 제2항	
		정보통신망법 제64조의5(투명성 보고서 제출의무 등), 제76조(과태료) 제3항	
		전기통신사업법 제22조의5(부가통신사업 자의 불법촬영물 등 유통방지)	
	정부시책 마련	정보통신망법 제4조(정보통신망 이용촉진 및 정보보호등에 관한 시책의 마련) 제1,2항, 제44조(정보통신망에서의 권리보호) 제3항	

국내 제도 현황 및 개선 논의	구분	내용	
	사후규제방안	위터마크 표시의무 제도	○ 정보통신망법 제44조의7 제1 항 각 호에 위터마크 표시의무, 변경내용 표시의무 관련 내용 추가
		딥페이크 변경내용 표시의무제도	○ 정보통신망법 제74조 제1항 각 호에 위반시 형사처벌 규정 추가
	딥페이크 피해자의 구제강화 방안	피해자의 삭제요구권 강화	○ 정보통신망법 제44조의2 제1 항 개선
		국내대리인 지정 제도의 활용	○ 해외 소규모 사업자에의 적 용을 위해 국내대리인 지정 제 도의 기준 완화 고려
	딥페이크 식별 기술의 지원	딥페이크 식별 및 인증을 위한 기관 지정 또는 설립 근거규정 마련	○ 정보통신망법 상 인공지능 기술을 이용한 거짓정보 식별 및 인증을 위한 기관 지정 또는 별도 기관 설립에 관한 규정 신설
		딥페이크 식별 기술 및 재정 지원을 위한 근거규정 마련	○ 정보통신망법 상 인공지능 기술을 이용한 거짓정보 식별 기술의 개발 지원, 재정지원에 관한 규정 신설
	딥페이크 관련 전담부서 및 범부처협의체의 운영	전담부서 운영	추후 지정 필요
		범부처협의체 운영	추후 구성 필요 (방송통신위원회, 과학기술정보통신부, 법무부, 경찰청, 여성가족부, 선거관리위원회 등)

참 고 문 헌

국내 문헌

- 국경완(2019. 6. 12), 『블록체인 기술 및 산업 분야별 적용 사례』, 정보통신기획평가원 주간기술동향.
- 김현수, 권혁준(2018. 12. 10), 『보험 산업의 블록체인 활용』, 보험연구원.
- 저작권위원회(2019. 2.), 『저작권기술 동향』, 저작권위원회.
- 정보통신정책연구원(KISDI)(2010. 12.), 『방송통신 진화에 따른 규제체계 고도화방안 연구』.
- 박용상(2010), 『헌법상 사전검열금지의 원칙』, 법학논집 제21호.
- 심재철, 오미영(2011), 『방송통신심의위원회의 위상과 나아갈 방향에 대한 시론』.
- 강상익(2001), 『디지털 워터마킹 국내·외 표준화 동향』, TTA저널 제73호.
- 오병택·문병주·이동일(2002), 『디지털 워터마킹 기술동향 및 전망』, 전자통신동향분석 제17권 6호.
- 김유향(2019. 10.), 『딥페이크(Deepfake)의 발전과 해외 법제도 대응』, 국회입법조사처 이슈와 논점.
- 이동후 外(2016. 10.), 『스마트 미디어 시대 인터넷 개인방송 규제 체계 정비』, 국회입법조사처.
- 방송통신위원회(2019. 3.), 『국내대리인 지정제도 안내서』.
- 방송통신위원회·한국인터넷진흥원(2013. 2.), 『사업자를 위한 올바른 백신 프로그램 배포 가이드』, 방송통신위원회.

- J.-Y. Zhu*, T. Park*, P. Isola, A. A. Efros: Unpaired Image-to-Image Translation using Cycle-Consistent Adversarial Networks. ICCV 2017
- F. Schroff, D. Kalenichenko, J. Philbin: FaceNet: A unified embedding for face recognition and clustering. CVPR 2015
- J. S. Chung, A. Senior, O. Vinyals, A. Zisserman: Lip reading sentences in the wild. CVPR 2017
- S. Suwajanakorn, S. Seitz, I. Kemelmacher-Shlizerman: Synthesizing Obama: learning lip sync from audio. ACM Transactions on Graphics (TOG), 36(4), 2017
- D. Wen, H. Han, A. K. Jain: Face spoof detection with image distortion analysis. IEEE Transactions on Information Forensics and Security, 10(4), 746–761, 2015
- P. Zhou, X. Han, V. I. Morariu, L. S. Davis: Two-Stream Neural Networks for Tampered Face Detection. CVPR Workshops 2017
- E. Sabir, J. Cheng, A. Jaiswal, W. AbdAlmageed, I. Masi, P. Natarajan: Recurrent Convolutional Strategies for Face Manipulation Detection in Videos. CVPR Workshops 2019
- S. Sabour, N. Frosst, G. E. Hinton: Dynamic routing between capsules. NIPS 2017
- A. Rössler, D. Cozzolino, L. Verdoliva, C. Riess, J. Thies, and M. Nießner, “FaceForensics++: Learning to Detect Manipulated Facial Images,” in Proc. IEEE/CVF International Conference on Computer Vision, 2019.
- Y. Li, X. Yang, P. Sun, H. Qi, and S. Lyu, “Celeb-DF: A Large-Scale Challenging Dataset for DeepFake Forensics,” in Proc. IEEE/CVF Conference on Computer Vision and Pattern Recognition, 2020

홈페이지

<https://github.com/rcmalli/keras-vggface>
<https://github.com/shaoanlu/faceswap-GAN>
<https://www.bbc.co.uk/bitesize/articles/zfkwcqt>
<https://www.malavida.com/en/soft/fakeapp/>
<https://www.youtube.com/channel/UCsxwjK5ELsIXWs62jqBCAbA>
<https://www.youtube.com/watch?v=0sR1rU3gLzQ>
<https://ai.googleblog.com/2019/09/contributing-data-to-deepfake-detection.html>
<https://lingzhili.com/FaceShifterPage/>
<https://github.com/deepfakes/faceswap>
<https://www.aitimes.kr/news/articleView.html?idxno=17581>
<https://ai.facebook.com/datasets/dfdc/>
https://github.com/selimsef/dfdc_deepfake_challenge
<https://www.sciencetimes.co.kr/news/%EB%B8%94%EB%A1%9D%EC%B2%B4%EC%9D%B8%EC%9C%BC%EB%A1%9C-%EB%94%A5%ED%8E%98%EC%9D%B4%ED%81%AC-%EB%8C%80%EC%9D%91%ED%95%A0-%EC%88%98-%EC%9E%88%EC%96%B4/>
<https://ambervideo.co/#>
<https://www.congress.gov/bill/115th-congress/senate-bill/3805/text?format=txt>
https://nyassembly.gov/leg/?default_fld=&leg_video=&bn=A08155&term=2017&Text=Y
https://nyassembly.gov/leg/?default_fld=&leg_video=&bn=A08155&term=2017&Summary=Y
https://nyassembly.gov/leg/?default_fld=&leg_video=&bn=S05959&term=2019&Text=Y
<https://malegislature.gov/Bills/191/H3366.Html>
https://www.wilmerhale.com/-/media/files/shared_content/editorial/publications/wh_publications/client_alert_pdfs/20190925-deepfake-legislation-a-nationwide-survey.pdf

https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201920200AB602
https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201920200AB730
<http://www.aitimes.com/news/articleView.html?idxno=120085>
<https://www.billtrack50.com/BillDetail/1174065>
<https://ec.europa.eu/digital-single-market/en/news/communication-tackling-online-disinformation-european-approach>
<https://ec.europa.eu/digital-single-market/en/news/code-practice-disinformation>
https://ec.europa.eu/commission/publications/action-plan-disinformation-commission-contribution-european-council-13-14-december-2018_en
https://eeas.europa.eu/sites/eeas/files/joint_report_on_disinformation.pdf ·
https://www.legifrance.gouv.fr/download/pdf?id=6-nJtAIQpD8-Ugn4wumM7q3PzXyh2U2x_naRfEud_Wg=
https://www.legifrance.gouv.fr/codes/texte_lc/LEGITEXT000006070239/2020-09-17/
<https://www.legifrance.gouv.fr/loda/id/LEGITEXT000006068930/2020-09-17/>
<https://www.legifrance.gouv.fr/loda/id/LEGITEXT000006070722/2020-09-17/>
<https://www.gesetze-im-internet.de/netzdg/BJNR335210017.html>
<https://www.nhk.or.jp/kokusaihoudou/archive/2020/04/0408.html>
<https://www.edaily.co.kr/news/read?newsId=01498966625738416&mediaCodeNo=257&OutLinkChk=Y>
http://www.dt.co.kr/contents.html?article_no=2020100202109919607005&ref=naver
<https://www.hankyung.com/society/article/202003275942H>
https://biz.chosun.com/site/data/html_dir/2020/10/05/2020100502248.html
<https://webcache.googleusercontent.com/search?q=cache:kFEFNcB89UgJ:https://www.wired.com/story/detect-deepfakes-camera-watermark/+&cd=1&hl=ko&ct=clnk&gl=kr>
<http://www.hani.co.kr/arti/PRINT/897415.html>
http://privacy.or.kr/wp-content/uploads/2003/04/PT_20021128_LJH.hwp

<https://www.aitimes.kr/news/articleView.html?idxno=18184>
<https://dacon.io/competitions/official/235655/overview/>
<https://www.sciencetimes.co.kr/news/%EB%B8%94%EB%A1%9D%EC%B2%B4%EC%9D%B8%EC%9C%BC%EB%A1%9C-%EB%94%A5%ED%8E%98%EC%9D%B4%ED%81%AC-%EB%8C%80%EC%9D%91%ED%95%A0-%EC%88%98-%EC%9E%88%EC%96%B4/>
<https://m.etnews.com/20200621000057>
<https://blogs.microsoft.com/on-the-issues/2020/09/01/disinformation-deepfakes-newsguard-video-authenticator/>
https://www.boho.or.kr/download/dedicatedVaccine/downloadView.do?bulletin_writing_sequence=26603
https://www.boho.or.kr/data/guideView.do?bulletin_writing_sequence=1885
https://kcc.go.kr/user.do;jsessionid=lyCNqrenAGvyNHSLvaynqccV49SellIWL7OcVB8DwcbCX8quVmdm0JymN2Z4o2a2.hmpwas01_servlet_engine1?mode=view&page=A02060400&dc=K02060400&boardId=1030&cp=1&boardSeq=50070

● 저 자 소 개 ●

김 경 환

- 서울대 전기공학과 졸업
- 서울대 공과대학원 전기공학과 석사
- 사법시험 제46회 합격
- 입법고시 제18회 합격
- 사법연수원 제36기 수료
- 현 법무법인 민후 대표변호사

양 진 영

- 서울대 법학과 졸업
- 사법시험 제52회 합격
- 사법연수원 제42기 수료
- 현 법무법인 민후 변호사

방송통신융합 정책연구 KCC-2020-15

딥페이크 기술 대응 법제도 개선 방안 연구

2020년 월 일 인쇄

2020년 월 일 발행

발행인 방송통신위원회 위원장

발행처 방송통신위원회

경기도 과천시 관문로 47

정부과천청사 2동

TEL: 02-2110-1323

Homepage: www.kcc.go.kr

