인공지능 및 개인정보보호

~에 의해

다니엘 J. 솔로베

초안: 2024년 2월 1일

추상적인

이 기사는 인공지능(AI)과 개인정보 보호의 교차점에 대한 근본적인 이해를 확립하고, AI가 개인정보 보호에 제기하는 현재 문제를 간략하게 설명하고 이 분야에서 법의 발전을 위한 잠재적인 방향을 제시하는 것을 목표로 합니다. 지금까지 AI와 개인 정보 보호가 어떻게 상호 연관되는지에 대한 전반적인 환경을 탐구한 논평가는 거의 없습니다. 이 기사에서는 이 영역의 지도를 작성하려고 합니다.

일부 평론가들은 개인정보 보호법이 AI 문제를 해결하는 데 적합한지 의문을 제기합니다. 이 글에서 나는 기존의 개인 정보 보호법이 AI의 개인 정보 보호 문제를 해결하는 데는 훨씬 부족하지만 적절하게 개념화되고 구성된 개인 정보 보호법은 이를 해결하는 데 큰 도움이 될 것이라고 주장합니다.

개인 정보 보호 문제는 AI의 입력과 출력에서 나타납니다. 이러한 개인 정보 보호 문제는 종종 새로운 것이 아닙니다. 이는 오랫동안 지속된 개인 정보 보호 문제의 변형입니다. 그러나 AI는 기존의 개인 정보 보호 문제를 복잡하고 독특한 방식으로 재구성합니다. 일부 문제는 기존 규제 체계에 도전하는 방식으로 혼합되어 있습니다. 많은 경우 AI는 기존 문제를 악화시키며 종종 문제를 전례 없는 수준으로 끌어올리겠다고 위협합니다.

전반적으로 AI는 개인 정보 보호에 대한 예상치 못한 격변이 아닙니다. 여러 면에서 오랫동안 예측되어 온 미래입니다. 그러나 AI는 기존 개인정보 보호법의 오랜 단점, 허점, 잘못된 접근방식을 노골적으로 드러냅니다.

궁극적으로 AI가 영향을 미치는 개인 정보 보호 문제를 해결하려면 기존 법률에 대한 패치를 통해든 새로운 법률의 일부로든 많은 문제를 해결해야 합니다.
이 기사에서는 법이 다루어야 하는 주요 문제에 대한 로드맵과 작동할 수 있는 접근 방식과 실패할 접근 방식에 대한 지침을 제공합니다.

인공 지능 및 개인 정보 보호

다니엘 J. 솔로브1

Barbara A. Bernard 조지워싱턴대학교 로스쿨 지적재산권 및 기술법 교수.

소개

> 예술과 과학이 경이로운 모습으로 만나고 기계가 자신의 생각을 갖게 되면 마음과 눈을 가득 채우는 두려움이 있습니다. 한 때 소중하게 여겨졌던 사생활은 사라질 것입니다.
>
> -채팅GPT

인공지능(AI)이 마법같은 순간을 맞이하고 있습니다. AI는 어디에나 있고 모두가 그것에 대해 이야기하는 것 같습니다. AI가 전 세계적으로 빠르게 발전하고 삶의 거의 모든 측면에 침투하면서 지적 재산, 고용, 안전, 특히 개인 정보 보호에 이르기까지 수많은 문제를 야기합니다.

상황을 더욱 복잡하게 만드는 AI는 다양한 방식으로 개인 정보 보호에 영향을 미치고 수많은 우려를 불러일으킵니다.

이 글에서는 AI와 개인 정보 보호의 관계를 이해하는 방법에 대한 개념적, 실무적 기반을 마련하고 개인 정보 보호법이 AI를 어떻게 규제해야 하는지에 대한 로드맵을 제공하는 것을 목표로 합니다. 지금까지 AI와 개인 정보 보호가 어떻게 상호 연관되는지에 대한 전반적인 환경을 탐구한 논평가는 거의 없습니다. 이 기사에서는 이 영역의 지도를 작성하려고 합니다.

기존 개인정보 보호법은 이미 "자동화된" 데이터 처리에 관한 몇 가지 조항이 있는 유럽 연합의 일반 데이터 보호 규정(GDPR)과 같이 AI를 어느 정도 다루고 있습니다. 2 미국의 여러 주 소비자 개인 정보 보호법에도 자동화에 대한 조항이 있지만 그 범위가 좁고 제한적입니다. 삼

AI에만 초점을 맞춘 새로운 법률이 곧 등장할 예정입니다. EU는 최근 AI법을 제정했습니다.4 AI법은 미국에서 싹트기 시작했습니다5

개인 정보 보호법이 이러한 문제를 규제하는 데 적합한 도구입니까? 아니면 AI의 사생활인가?
전문 AI 법률에 의해 가장 잘 규제되는 문제는 무엇입니까? 일부 평론가들은 개인정보 보호법이 AI 문제를 해결하는 데 적합한지 의문을 제기합니다. 법학 교수 Eric Goldman은 다음과 같이 주장합니다.

> 개인 정보 보호 옹호자들에게는 개인 정보 보호법의 범위가 계속 확대되는 것이 좋은 것처럼 들릴 수 있습니다. 나머지 우리에게는 의심할 여지 없이 좋은 일이 아닙니다. 우리는 개인 정보 보호 전문가가 자신의 범위 밖의 주제에 대해 정책 결정을 내리는 것을 원하지 않습니다. 그들은 필요한 전문 지식이 부족하므로 심각한 문제를 일으킬 것입니다.

---

[2] GDPR 예술. 22.

3 아래 X를 참조하세요.

4 EU 의회, 인공 지능법: 신뢰할 수 있는 AI를 위한 포괄적인 규칙에 대한 거래, 2023년 12월 9일, https://www.europarl.europa.eu/news/en/press-room/20231206IPR15699/ 신뢰할 수 있는 AI를 위한 포괄적인 규칙에 대한 인공 지능 행위 거래.

5 전국 주 의회 회의, 인공 지능 2023 법안(2024년 1월 12일), https://www.ncsl.org/technology-and-communication/artificial-intelligence-2023-legislation.

피할 수 있는 정책 오류.6

이 글에서 나는 기존의 개인 정보 보호법이 AI의 개인 정보 보호 문제를 해결하는 데는 훨씬 부족하지만 적절하게 개념화되고 구성된 개인 정보 보호법은 이를 해결하는 데 큰 도움이 될 것이라고 주장합니다.

법이 AI와 개인 정보 보호를 어떻게 규제해야 하는지 결정하려면 몇 가지 근본적인 문제를 검토하고 설명해야 합니다. 먼저 AI가 무엇인지 이해하는 것이 중요하다. 이 문제는 오늘날 "AI"라고 불리는 것이 오랫동안 일반적인 이해에서 의미했던 용어가 아니기 때문에 복잡합니다.

지각있는 로봇. 이제 'AI'라는 용어는 기계 학습 알고리즘 및 관련 기술을 설명하는 데 사용되며 스스로 생각할 수 있는 기계와는 다릅니다. 오늘날의 AI는 매우 흥미롭게도 오래되고 새롭습니다. 이는 오랜 진화의 한 단계이자 중요한 도약이기도 합니다. 오늘날 AI 기술의 대부분은 개인 정보 보호법에 잘 알려져 있으며, 이러한 기술이 개인 정보 보호에 영향을 미치는 방식은 그다지 놀라운 일이 아닙니다.

둘째, AI가 제기하는 개인정보 보호 문제를 이해해야 합니다. 법이 어떻게 규제해야 하는지, 기존 법이 부족한 부분은 무엇인지, 법에 어떤 변경이나 추가가 이루어져야 하는지 결정하려면 큰 그림을 이해하는 것이 중요합니다. AI에는 입력을 소비하고 출력을 생성하는 알고리즘이 포함됩니다.

개인 정보 보호 문제는 입력과 출력 모두에서 나타납니다. 이러한 개인 정보 보호 문제는 종종 새로운 것이 아닙니다. 이는 오랫동안 지속된 개인 정보 보호 문제의 변형입니다.7 그러나 AI는 기존의 개인 정보 보호 문제를 복잡하고 독특한 방식으로 재구성합니다. 일부 문제는 기존 규제 체계에 도전하는 방식으로 혼합되어 있습니다. 많은 경우 AI는 기존 문제를 악화시키며 종종 문제를 전례 없는 수준으로 끌어올리겠다고 위협합니다.

입력 문제에는 데이터 수집 문제가 포함되며, 여기에는 스크레이핑(동의되지 않은 온라인 데이터 수집)과 보다 합의된 형태의 데이터 수집이 포함됩니다. 두 가지 형태의 데이터 수집 모두 대부분의 개인 정보 보호법에서 제대로 다루어지지 않습니다.

AI 결과물의 개인 정보 보호 문제에는 데이터 생성, 의사 결정 및 데이터 분석이 포함됩니다. 추론을 통해 생성된 새로운 데이터는 사람들이 기대하지 않거나 공개하고 싶지 않은 세부 정보를 공개할 수 있습니다. 데이터 생성은 데이터 수집과 데이터 처리 사이의 경계를 모호하게 하여 많은 개인 정보 보호법 보호를 둘러싼 최종 실행을 가능하게 합니다.

AI 데이터 생성은 전례 없는 규모로 악의적인 자료를 생성할 수도 있으며, 이는 사기 및 조작과 관련된 문제를 악화시킬 수 있으며,

---

6 Eric Goldman, 개인정보 보호법은 인터넷법(및 기타 교리)을 삼키고 있습니다...모든 사람에게 해를 끼치고 있습니다. 기술 및 마케팅 법률 블로그(2023년 5월 9일), https://blog.ericgoldman.org/archives/2023/05/privacy- 법은 삼키는 인터넷법과 기타 교리-모든 사람에게 해를 끼치는 것입니다.htm.

7 나는 이전에 다양하면서도 관련된 개인 정보 보호 문제에 대한 광범위한 분류 체계를 개발했습니다. Daniel J. Solove, 개인 정보 보호 분류, 154 U. Pa. L. Rev. 477(2006)을 참조하십시오 .

새로운 데이터 보안 취약점을 만듭니다. 악의적이지 않은 AI 콘텐츠라도 AI가 특정 상황에서 인간을 시뮬레이션하는 경우처럼 기만적이고 조작적일 수 있습니다.

AI 결과의 또 다른 세트에는 AI 알고리즘을 사용하여 사람에 대한 결정을 내리는 것이 포함됩니다. AI는 사람들의 미래 행동을 예측할 수 있으며, 이는 사람들이 아직 수행하지 않은 일에 대한 개입과 판단으로 이어질 수 있으며, 인간 주체에 대한 존중을 감소시킬 수 있습니다. AI 의사결정의 자동화는 이를 개인화하여 정량화 가능한 차원으로 치우치고 정량화할 수 없는 사람에 대한 고유한 세부 정보에서 멀어지게 합니다. AI는 또한 결정에 편견을 체계적으로 인코딩할 수 있습니다.

또한 AI 데이터 분석은 감시 및 식별과 같은 개인정보 침해 사례를 확대하여 감시자의 권한과 통제력을 강화할 수 있습니다.

AI는 규제 감독, 이해관계자 참여 및 책임에 대한 까다로운 문제를 제기합니다. AI 알고리즘은 역동적이고 종종 이해하기 어렵기 때문에 AI는 투명성을 심각하게 복잡하게 만듭니다. AI는 개인의 정당한 절차에 대한 과제를 제시합니다. AI 기술의 개발은 영향을 받는 많은 이해관계자 그룹, 특히 대표성이 낮고 소외된 그룹을 배제하는 경우가 많습니다.

AI에 대한 적절한 책임이 부족한 경우가 많습니다. 성공적인 AI 기술 개발에 대한 엄청난 높은 보상으로 인해 규제 집행이 압도되는 경우가 많아 확인되지 않은 위험 감수로 이어지는 경우가 많습니다. 알고리즘 파괴와 같은 구제책은 실제로 구현하기 어렵습니다.

전반적으로 AI는 개인 정보 보호에 대한 예상치 못한 격변이 아닙니다. 여러 면에서 오랫동안 예측되어 온 미래입니다. 그러나 AI는 기존 개인 정보 보호법의 오랜 단점, 허점, 잘못된 접근 방식을 극명하게 드러냅니다.

궁극적으로 AI가 영향을 미치는 개인 정보 보호 문제를 해결하려면 기존 법률에 대한 패치를 통해든 새로운 법률의 일부로든 많은 문제를 검토해야 합니다.
AI는 지각 있는 기계를 포함하지 않음에도 불구하고 엄청나게 강력하고 혁신적인 기술 세트이기 때문에 위험이 높습니다. 이 기사에서는 법이 다루어야 할 주요 문제에 대한 로드맵과 효과가 있는 접근법과 실패할 접근법에 대한 지침을 제공할 것입니다.

1부에서는 AI가 무엇인지, AI가 아닌지에 대해 논의하고, 신화를 없애고, AI가 오래되고 새로운 이유를 설명하고, AI 개인 정보 보호 문제를 다른 개인 정보 보호 문제와 별도로 취급해야 할 만큼 고유한 것으로 보는 "AI 예외주의"에 대해 조언합니다.
2부에서는 AI 및 개인 정보 보호 규제에 대한 로드맵을 제시합니다. AI가 제기하는 개인 정보 보호 문제를 살펴보고 법이 어떻게 대응해야 하는지 논의합니다.

I. AI: 오래된 것은 다시 새로운 것입니다

충분히 발전된 기술은 마법과 구별할 수 없습니다.

— 아서 C. 클라크8

AI 전문가 Mustafa Suleyman은 “AI는 다른 기술보다 훨씬 더 깊고 강력합니다.”라고 단언합니다. “위험은 그것을 과장하는 데 있는 것이 아닙니다. 오히려 다가오는 파도의 크기를 놓치는 것입니다. 이는 단순한 도구나 플랫폼이 아니라 혁신적인 메타 기술입니다.”9

AI와 관련된 개인 정보 보호 문제와 규제 방법을 이해하려면 AI가 무엇인지, 아닌지를 이해하는 것이 필수적입니다. AI는 오해의 소지가 있는 용어와 은유로 인해 현재 AI에 대한 상당한 혼란이 팽배합니다.

A. AI 의 부상

인공지능은 지능형 로봇의 이미지와 SF적 환상을 불러일으킨다.
수백 년 동안 공상과학 소설은 인간의 창조를 상상해왔습니다.
Mary Shelley의 소설에서 버림받은 괴물과 같은 지각 있는 존재와 기계
프랑켄슈타인; 또는 Modern Prometheus (1818)부터 그의 책 I, Robot (1950) 에 수집된 1940년대
Isaac Asimov의 로봇 이야기, 영화 2001: A Space Odyssey (1968) 의 차갑고 살인적인 HAL, 친절하지만 성가신 C3PO까지 스타워즈 (1977) 에서는 터미네이터 (1984) 의 무시무시한 사형 집행 로봇, 스타트렉: 넥스트 제너레이션 (1987) 의 인간과 유사한 합성 데이터, Her (2013) 의 부드러운 디지털 비물리적 로봇까지 말입니다 . 이 작품들은 대중의 의식을 사로잡는다. 많은 사람들은 AI가 마침내 페이지와 화면을 뛰어넘어 현실이 되는 날을 간절히 (그리고 때로는 떨리게) 기다려왔습니다.

그러나 그것은 일어나지 않았습니다. 20세기 중반부터 메인프레임 컴퓨터, 가정용 컴퓨터, 노트북 컴퓨터, 스마트폰 등이 등장하면서 디지털 혁명이 시작되었습니다. 우리는 인터넷의 부상, 컴퓨팅 성능의 기하급수적인 성장, 데이터 저장 용량의 광대한 확장, 빅 데이터의 힘증가, 사물 인터넷의 부상을 목격했습니다. 그러나 AI는 공상과학의 영역에 머물렀다. . . 최근까지.

컴퓨터 과학자 John McCarthy는 1955년 Dartmouth에서 "인공 지능"이라는 용어를 만들었습니다.10
10년 내내 AI를 개발하려는 많은 시도가 있었습니다.

---

8 Eric Siegel, Why AI Is a Big Fat Lie, Big Think, 2019년 1월 23일 에서 인용 .

9 무스타파 술레이만 (MUSTAFA SULEYMAN), 다가오는 물결 : 기술, 권력, 그리고 21 세기 최대 딜레마 78(2023).

10 크리스 위긴스와 매튜 L. 존스, 데이터가 어떻게 발생했는지: 이성 의 시대 부터 알고리즘 시대 까지 의 역사 126-27(2023).

이후 수십 년이 걸렸지만 이러한 노력은 대개 실망으로 끝났습니다.11 1973년 영국의 수학자 제임스 라이트힐 경(Sir James Lighthill)은 자신의 기사인 인공 지능: 일반 조사(Artificial Intelligence: A General Survey) 에서 다음과 같이 유명하게 선언했습니다. 그때 약속이 있었죠."12

브라이언 크리스찬(Brian Christian)이 말했듯이, "인공지능의 역사는 희망과 우울이 교차하는 순환의 하나로 유명합니다."13

기술 저널리스트인 Meredith Broussard에 따르면 금세기 첫 10년 동안 주류 대중은 "대부분 AI를 무시했습니다." 그런데 2010년대 중반부터 "사람들은 머신러닝에 대해 이야기하기 시작했습니다. 갑자기 AI가 다시 불타올랐습니다."14 Broussard는 2017년을 AI의 인기가 높아지기 시작한 해로 꼽았습니다.

오늘날 AI 열풍을 촉발한 불꽃은 프롬프트에 대한 텍스트 응답을 생성할 수 있는 기계 학습 대규모 언어 모델인 ChatGPT입니다. ChatGPT는 기술 리더와 투자자 그룹이 2015년에 출시한 Open.AI에 의해 개발되었습니다. 원래 비영리였던 Open.AI는 2019년에 영리 회사가 되었습니다. 2021년 Open.AI는 ChatGPT를 대중에게 공개했습니다.15

ChatGPT의 성공에 영감을 받아 다른 많은 회사에서도 유사한 AI 도구를 출시했습니다. 그 소문은 금세 열풍으로 변했습니다. 이제 드디어 AI의 시대가 도래한 것 같습니다.

B. AI 란 무엇 인가 ?

오늘날 사용되는 "AI"라는 용어는 공상 과학 소설에 나오는 것과 같은 자기 인식 로봇의 생성 이상의 것을 포함합니다. 대신, 알고리즘과 관련된 광범위한 기술이 필요합니다. 알고리즘은 작업을 수행하기 위한 명령 또는 지침의 집합입니다. 알고리즘은 수학적 방법과 유사합니다.

AI는 문제 해결, 의사 결정, 언어 이해, 인식 등 일반적으로 인간의 지능이 필요한 작업을 수행할 수 있는 컴퓨터 시스템의 개발을 의미합니다. 법학 교수 Ryan Calo는 다음과 같이 지적합니다. "인공 지능에 대한 간단하고 합의된 정의는 없습니다. AI는 기계를 사용하여 인간이나 동물 인지의 일부 측면을 근사화하는 것을 목표로 하는 일련의 기술로 가장 잘 이해됩니다." 16

---

11 ID. 182에서.

12 WIGGINS AND JONES, HOW DATA HAPPENED, 각주 X, 182쪽.

13 브라이언 크리스티안, 정렬 문제: 기계 학습과 인간 의 가치 20(2020).

14 메러디스 브루사드, 인공 비지능: 컴퓨터가 세상을 오해하는 방법 90 (2018).

15 Rebecca Barker, "ChatGPT에 두뇌가 있었다면 이런 모습이었을 것입니다." Fast Company(2023년 8월 17일), https://www.fastcompany.com/90940143/if-chatgpt-had-a- 두뇌는 이것이 어떻게 보일지입니다.

16 Ryan Calo, 인공 지능 정책: 입문서 및 로드맵, 51 UC Davis L. Rev. 399, 404 (2017).

1. 기계 학습, 신경망 및 생성 AI

현대 AI의 핵심에는 머신러닝 알고리즘이 있습니다. 오늘날 "AI"라는 용어의 대부분의 사용은 기계 학습을 의미합니다. 이러한 알고리즘은 지능을 시뮬레이션할 수 있지만 실제로는 지능적이지 않습니다.

기계 학습 알고리즘은 데이터를 기반으로 추론이나 예측을 수행합니다.
이러한 알고리즘은 "훈련 데이터"라고 불리는 점점 더 많은 양의 데이터가 입력됨에 따라 개선되고 발전합니다. 컴퓨터 "프로그래머는 사용할 기계 학습 모델을 선택하고, 데이터를 제공하며, 컴퓨터 모델이 스스로 훈련하여 패턴을 찾거나 예측하도록 합니다." 기계 학습 알고리즘은 방대한 양의 데이터에 의존합니다. “데이터가 많을수록 프로그램은 더 좋아집니다.”17

"신경망"이라고 불리는 기계 학습의 한 유형에는 "딥 러닝" 알고리즘이 포함됩니다. 신경망은 "인간의 뇌에서 영감을 받아 생물학적 뉴런이 서로 신호를 보내는 방식을 모방"합니다. 18 신경망은 인공 뉴런처럼 작동하도록 설계된 "노드"라고 불리는 다양한 계층을 통해 작동합니다. 각 노드는 다른 노드와 연결되어 있으며 할당된 가중치와 임계값을 가지고 있습니다. 노드의 출력이 이 임계값을 초과하면 노드가 활성화되어 네트워크의 다음 계층으로 데이터를 전송합니다. 그렇지 않으면 비활성 상태로 유지되어 데이터 흐름이 중단됩니다.

현재 AI에 대한 대중의 관심은 텍스트, 음성, 이미지, 비디오 등 새로운 콘텐츠를 전문적으로 생성하는 인공 지능의 한 분야인 생성 AI에 관한 것입니다. 생성 AI의 예로는 ChatGPT와 같은 LLM(대형 언어 모델) 챗봇이 있습니다. 사용자는 생성 AI가 응답을 생성하여 응답하는 "프롬프트"(쿼리 또는 요청)를 입력하여 이러한 AI 도구와 상호 작용합니다. ChatGPT는 DALL-E라는 이미지 생성 도구와 통합되어 있습니다. 제너레이티브 AI는 수신된 프롬프트를 기반으로 새롭고 관련성이 높은 출력을 생성할 수 있습니다.

AI와 자동화는 종종 함께 언급되지만 동일한 것은 아닙니다. AI는 자동화의 한 형태이지만, "자동화"라는 용어는 "장치, 프로세스 또는 시스템을 자동으로 작동시키는 기술"을 더 광범위하게 포함합니다. 19 많은 형태의 자동화에는 데이터가 포함되지 않으며, 자동화된 처리는 데이터를 포함하지 않습니다. 데이터를 포함하지만 많은 형태에는 현재 AI라고 불리는 유형의 기계 학습 알고리즘이 포함되지 않습니다.

---

17 Sara Brown, 기계 학습, 설명, MIT Sloan 경영 대학원(2021년 4월 21일), https://mitsloan.mit.edu/ideas-made-to-matter/machine-learning-explained.

18 IBM, 신경망이란 무엇입니까? https://www.ibm.com/topics/neural-networks.

19 Merriam-Webster 사전, 자동화, webster.com/dictionary/ https://www.merriam-automation.

2. 기존 기술의 브랜드 변경

오늘날 AI에 대한 논의를 혼란스럽게 만드는 것은 AI가 머신러닝 기술의 브랜드를 바꾸는 데 사용되는 용어라는 점입니다. 머신러닝 전문가인 Eric Siegel은 "AI는 큰 거짓말입니다."라고 단언했습니다. AI는 “혼란시키고 속이는 과장된 유행어이다. . . . AI는 브랜드일 뿐이다. 강력한 브랜드이지만 공허한 약속입니다.”20 Siegal에 따르면, “[현재 AI라고 명명된 기술에 대한] 훨씬 더 정확하고 정확한 용어는 일반적으로 기계 학습 입니다 . 정말 강력합니다.”21

머신러닝은 새로운 것이 아닙니다. 사실 약 80년 동안 개발된 오래된 기술이다. 1943년에 신경학자 Warren McCulloch와 논리학자 Walter Pitts는 A Logical Calculus of Ideas Immanent in Nervous Activity 라는 제목의 논문을 발표했습니다 . 그들은 이 논문이 신경과학에 영향을 미칠 것이라고 생각했지만 대신 신경망의 기본 아이디어를 담고 있었습니다.22 다음으로 중요한 발전은 1949년에 출판된 Donald Hebb의 저서 The Organisation of Behavior: A Neuropsychological Theory 였습니다 .

1957년에 심리학자 Frank Rosenblatt는 최초의 신경망으로 칭송받는 거대한 컴퓨터인 "퍼셉트론"이라는 기계를 개발했습니다.23 이 기계는 New York Times 와 The New Yorker 에서 보도되었습니다. 지금까지 고안된 인간 두뇌에 대한 심각한 경쟁자입니다.”24 그러나 처음의 약속에도 불구하고 그 인식은 결국 무너진 기대로 끝났습니다. "현대 신경망에는 수백만 개의 레이어가 있지만 레이어가 하나뿐"이었기 때문에 실패했습니다.25

'머신러닝'이라는 용어는 1959년부터 사용되기 시작했습니다. 26 그러나 기술의 발전은 느리고 전망도 미심쩍었습니다. 전설적인 컴퓨터 과학자 Marvin Minsky는 기계 학습의 실행 가능성에 대해 의구심을 갖고 1969년에 컴퓨터 과학자 Seymour Papert와 함께 당시 연구 방향에 의문을 제기하는 책을 출판했습니다.27 이 책의 결과는 "거의 연구가 거의 없었습니다. . . 이 분야에서는 약 1980년대까지” 그리고 “20년 넘게 전 세계에서 AI 연구에 대한 자금이 감소”했는데, 이 기간을 “AI의 첫 번째 겨울”이라고 합니다.28

---

20 Eric Siegel, AI가 큰 거짓말인 이유, Big Think, 2019년 1월 23일.

21 ID.

22 기독교인, 정렬 문제, 각주 X, 2-3.

23 Melanie Lefkowitz 교수의 퍼셉트론이 AI의 길을 열다 – 60년이 너무 빨리 다가옴, Cornell Chronicle(2019년 9월 25일), https://news.cornell.edu/stories/2019/09/professors-perceptron-paved-way- 아이-60년이 너무 빨리 왔네요.

24 ID.

25 ID.

26 BROUSSARD, 인공 비지능, 각주 X, at 91.

27 CHRISTIAN, 정렬 문제, 각주 X, 20-21.

28 Alexander L. Fradkov, 기계 학습의 초기 역사, 53 ScienceDirect 1385, 1387 (202).

그러나 머신러닝은 계속해서 발전했습니다. 돌파구는 1990년대에 일어났다. 기계 학습 전문가인 Eric Siegel은 1997년에 기계 학습 과정을 가르치기 시작했으며 "신경망은 이미 제한된 상황에서 자율 주행 자동차를 조종하고 있었습니다."라고 말했습니다.

21세기가 되면서 머신러닝이 등장했습니다. "머신러닝"이라는 용어는 2000년 옥스퍼드 영어 사전에 포함되었습니다.30 Alexander Fradkov가 지적했듯이 21세기 첫 10년은 "세 가지 동기적 추세", 즉 방대한 양의 데이터로 인해 발생한 머신러닝 역사의 "전환점"이었습니다. "병렬 컴퓨팅 및 메모리 비용" 감소 및 "심층 기계 학습의 새로운 알고리즘 개발"이 가능해졌습니다.31

우리가 AI를 통해 목격한 것은 실제로 머신러닝 기술의 등장과 혁신입니다. 수학자 Chris Wiggins와 역사학자 Matthew Jones는 "기계 학습, 특히 신경망을 사용하는 기계 학습은 기업 컨설턴트와 마케팅 담당자에 의해 AI로 이름이 바뀌었고 때로는 연구자들의 불편함을 야기했습니다."라고 주장했습니다.32 기계 학습이 개발될 당시 "생각한 사람은 거의 없었습니다. 이러한 노력을 'AI'로 간주합니다.”33

법학 교수인 Ryan Calo는 “오늘날 우리가 사용하는 [AI의] 거의 모든 기술은 . . Calo는 새로운 점은 "계산 능력과 교육 데이터에 대한 액세스가 크게 증가함에 따라 AI의 매우 중요한 분야인 기계 학습에서 실질적인 혁신이 이루어졌다"고 주장합니다 . 35 그리고 이제 Calo는 "정책 입안자들이 마침내 세심한 주의를 기울이고 있습니다"라고 말합니다.36

3. 오해를 불러일으키는 은유

AI는 기계 학습에 대한 오해의 소지가 있는 레이블이지만 기차는 역을 떠났고 돌아갈 수 없을 것 같습니다. 이제 AI는 마법의 유행어가 되었습니다. "아브라카다브라"라는 단어처럼 "AI"라는 용어를 사용하면 문이 열리고 투자자, 돈, 흥분 및 관심을 끌 수 있습니다. 결과적으로 기술 산업에서는 AI라는 라벨이 거의 모든 코드에 적용되고 있습니다. 요즘에는 실제로 AI로 간주되는 것이 무엇인지 아는 것이 어려울 수 있습니다.

AI는 용어이자 은유이다. 은유는 우리를 통해 렌즈 역할을 한다.

---

29 Eric Siegel, AI가 큰 거짓말인 이유, Big Think, 2019년 1월 23일.

30 메러디스 브루사드, 인공 비지능: 컴퓨터가 세상을 오해하는 방법 91 (2018).

31 Fradkov, Early History, 각주 X, at 1387.

32 WIGGINS AND JONES, HOW DATA HAPPENED, 각주 X, 190-91.

33 ID. 140에.

34 Ryan Calo, 인공 지능 정책: 입문서 및 로드맵, 51 UC Davis L. Rev. 399, 401-02(2017).

35 ID.

36 ID.

사물을 보고 해석하여 우리의 이해와 사고 과정을 형성하는 비교를 제공합니다. Ryan Calo가 통찰력 있게 관찰했듯이 "모든 은유는 그 자체로 논증입니다."37 은유는 우리의 인식을 명확하게 하고 왜곡시키는 이중 능력을 갖고 있으며 종종 이 두 가지 역할을 동시에 수행합니다.

오늘날 AI라고 불리는 것 중 실제로 지능적이거나 인공적인 것은 없습니다.38 AI는 본질적으로 수학에 데이터를 더한 것입니다. 기계 "학습"이라는 용어조차 오해의 소지가 있습니다. 기계는 인간처럼 학습하지 않기 때문입니다. '학습'이란 지식과 이해를 얻는 두뇌를 의미합니다. 기계 학습 알고리즘은 본질적으로 엄청난 양의 데이터를 공급받아 패턴을 인식합니다. Meredith Broussard가 설명했듯이, 기계 학습은 " 학습 이라는 용어가 암시하는 것과는 상관없이 기계가 지식이나 지혜 또는 선택 의지를 획득하는 것"이 아니라 "기계가 프로그래밍되고 일상적이며 자동화된 작업을 향상할 수 있다는 것을 의미합니다"39.

궁극적으로, 지각 있는 로봇에 대한 약속은 아직 실현되지 않았습니다. 그러나 오늘날 우리는 AI가 여기에 있다는 장엄한 선언을 듣습니다. 대신 관련 기술 세트가 마침내 잘 작동하기 시작했고 AI로 브랜드가 변경되었습니다.

은유는 기술에 인간과 같은 특성을 부여할 수 있지만 인간의 본질을 제거할 수도 있습니다. 우리의 장치는 단지 금속, 플라스틱, 유리의 집합체일 뿐이며, 데이터는 분리된 가상 공간에 떠다니는 것처럼 보입니다. 그러나 인간적 요소는 항상 기술에 필수적입니다. Kate Crawford가 언급했듯이 인간의 개입은 거의 모든 단계에서 AI에 깊이 내재되어 있습니다.40 AI 알고리즘을 훈련하는 데 사용되는 데이터는 인간의 활동, 생각, 대화에서 비롯되며 인간이 큐레이팅하는 경우도 많습니다. 인간은 알고리즘 모델을 설계하고 훈련하는 데 중요한 역할을 합니다 .41 Eric Siegel이 지적했듯이 가장 효과적인 기계 학습은 레이블이 지정된 훈련 데이터를 포함하는 "지도 기계 학습"입니다. 알고리즘은 레이블로부터 "학습"하여 레이블이 무엇인가 옳고 그른지 확인할 수 있습니다. 이 데이터에 라벨을 붙이는 것은 인간입니다.

AI는 천상의 것처럼 보이지만 근본적으로 물리적이며, 종종 힘들고 부담스러운 인간의 강렬한 노동에 뿌리를 두고 있으며 상당한 에너지와 물질적 자원에 의존합니다.42

실제로 오늘날의 AI는 발명 이후 유럽 청중을 사로잡은 체스 게임 기계인 Mechanical Turk와 대략적인 비유를 불러일으킬 수 있습니다.

---

37 Ryan Calo, 법적 은유로서의 로봇, 30 Harv. 제이엘앤테크. 209, 211(2016).

38 예브게니 모로조프, 인공지능의 문제? 인공적이지도 지능적이지도 않습니다, The Guardian(2023년 3월 30일).

39 메러디스 브루사드, 인공 비지능: 컴퓨터가 세상을 오해하는 방법 89 (2018).

40 케이트 크로포드, AI 아틀라스 : 권력, 정치, 인공 지능 의 지구적 비용 (2021); Rebecca Crootof, Margot E. Kaminski 및 W. Nicholson Price II, Humans in the Loop, 76 Vand. L. 개정 429(2023).

41 Margot E. Kaminski, 바이너리 거버넌스: 알고리즘 책임에 대한 GDPR 접근 방식의 교훈, 92 S. Cal. L. Rev. 1529, 1538-39 (2019).

42 CRAWFORD, ATLAS OF AI, 각주 X, 53-87; 이바나 바르톨레티, 인공 혁명: 권력 , 정치, AI 81-93(2020).

1770년과 그 후 거의 80년 동안. 나무 캐비닛과 상단에 체스판이 있는 이 장치는 한쪽 끝에 자동화된 터키 인형이 장착되어 있습니다. 그러나 그것은 결국 거짓임이 드러났다. 그 안에는 인간이 숨어 있었다.43 오늘날의 AI도 마찬가지로 인공과는 거리가 멀다.

인간의 노력과 깊이 연관되어 있다.

새롭고 익숙하지 않은 개념을 이해하기 위해 익숙한 개념에서 파생된 은유를 사용하는 것은 자연스럽고 피할 수 없는 경우가 많습니다. 은유 사용을 완전히 피할 수는 없지만, 우리가 선택한 은유와 그것이 우리의 이해에 가져올 수 있는 잠재적인 왜곡을 인식하는 것이 중요합니다.

AI에 사용되는 은유는 법률과 정책 형성에 큰 영향을 미칩니다.
AI와 관련된 개인 정보 보호 문제를 이해하려면 AI가 실제로 어떻게 작동하는지 이해하는 것이 중요합니다. AI를 위해 얼마나 많은 데이터가 수집되는지, 데이터가 어떻게 수집되는지, 데이터가 어떻게 형성되고 표준화되는지가 중요합니다. AI 도구가 출력을 생성하는 방법, 출력을 생성하는 AI 능력의 한계, 발생할 수 있는 잠재적인 오류 및 왜곡, 프로세스에서 손실되거나 변경되는 것이 중요합니다. AI는 현실을 정확하게 시뮬레이션하는 것이 아니라 변경하기 때문입니다. AI 도구를 어떻게 사용하는지가 중요합니다. AI 도구가 어떻게 설계되는지(무대 뒤의 인간, 동기, 목표, 편견 및 가정)가 중요합니다.

AI 사용자의 인식은 물론 AI의 결과에 어떻게 의존하는지도 중요합니다.
아이러니하게도 AI를 이해하는 방식은 AI를 인간과 유사한 특성으로 간주하여 의인화하고 인간 차원을 숨기는 방식으로 왜곡됩니다. 어느 방향으로든 왜곡되면 AI를 사용하고 규제하는 방식이 잘못될 수 있습니다.

우리가 AI를 이해하는 방식은 AI를 신뢰하는 정도, AI를 중립적이거나 편견으로 취급하는지, AI와 상호 작용하는 방식, 결정 및 기타 목적으로 AI를 사용하는 방식, 특정 문제를 인식하는지 여부, 이에 대한 책임을 누구에게 갖는지에 영향을 미칩니다. 궁극적으로 법의 대응은 AI에 대한 우리의 이해에 크게 좌우됩니다.

C. AI 예외주의 에 반대한다

개인 정보 보호 문제의 경우, 제가 "AI 예외주의"라고 부르는 것을 피하도록 주의해야 합니다.
AI를 매우 다르고 특별하게 다루기 때문에 AI의 개인 정보 보호 문제가 기존의 개인 정보 보호 문제와 어떻게 동일하고 단지 강화되었는지를 알 수 없습니다. AI는 오랫동안 기다려온 개인 정보 보호의 미래를 나타냅니다. AI는 현재 개인 정보 보호법의 뿌리 깊은 결함과 부적절함을 뚜렷이 강조하여 이러한 문제를 최우선으로 생각합니다.

AI는 정책 입안자들을 놀라게 하기 시작했습니다. 새로운 법률이 제안되고 있습니다. 비록 나는

43 Ifeoma Ajunwa, 반편향 개입으로서의 자동화의 역설, 40 Cardozo L. Rev. 1671, 1704-07(2020).

저는 이번 법개정의 기회를 확실히 받아들인다면, 새로운 법을 제정해야 할지, 기존 법을 바꿔야 할지에 대한 입장을 취하지 않습니다. 중요한 것은 정책 입안자가 AI와 관련된 개인 정보 보호 문제의 전체 상황에 대한 적절한 비전을 갖고 있는지 여부와 문제에 대한 적절한 이해 및 각 문제를 해결하는 방법을 가지고 있는지 여부입니다.

일부 평론가들은 AI 문제를 해결하기 위해 AI 특별법과 특별 기관이 필요하다고 요구하고 있습니다.44 추가 법률이 도움이 될 수 있지만 몇 가지 주의 사항이 있습니다. 첫째, 일반적인 AI 법률은 AI의 개인 정보 보호 문제에 충분히 초점을 맞추지 못해 많은 문제가 해결되지 않을 위험이 있습니다. AI는 필수적인 역할을 할 수 있는 기존 개인정보 보호법을 재검토하고 재고할 수 있는 기회를 제공합니다. 정책 입안자들은 개인 정보 보호법이 AI의 개인 정보 보호 문제를 처리하고 필요한 것은 추가 보호 계층뿐이라고 가정해서는 안 됩니다. 이런 실수를 하는 것은 기초가 불안정하고 제대로 설계되지 않은 건물에 이야기를 추가하는 것과 비슷할 것입니다.

AI의 개인 정보 보호 문제에는 개인 정보 수집 및 처리와 같은 개인 정보 보호법에서 오랫동안 다루어 온 관행이 포함됩니다. AI의 개인 정보 보호 문제에 직면하려면 이러한 관행을 AI 영역에 마치 평행 우주인 것처럼 어떤 마법의 선이 교차할 때뿐만 아니라 전체론적으로 함께 해결해야 합니다. AI는 디지털 시대 전반에 걸쳐 진행되어온 데이터 수집 및 사용과 지속적으로 연관되어 있습니다.

상업용 인터넷 초기에 Frank Easterbrook 판사는 별도의 "말의 법칙"이 없는 것처럼 인터넷도 별도의 법률에 의해 규제되어서는 안 된다고 유명하게 주장했습니다. 45 삶의 거의 모든 측면과 법률의 모든 영역에 영향을 미칠 인터넷과 같은 기술에 대해 새로운 전문법을 서두르지 말아야 한다는 점에서 그의 말은 부분적으로 옳습니다. AI는 그러한 기술일 가능성이 높습니다. 이는 엄청난 양의 문제에 영향을 미치고 수많은 법률 영역을 포함할 것입니다.46 그러나 이것이 AI에 특별한 고려가 필요한 차원과 문제가 부족하다는 의미는 아닙니다.

개인정보 보호를 위해 기존 법률이 사용되건, 새로운 법률이 사용되건, 혹은 조합되어 사용되건, 우리는 이제 결단의 순간에 이르렀습니다. 이 기사의 나머지 부분에서 설명하겠지만 기존 법률로는 해당 작업을 수행할 수 없습니다. 정책 입안자들이 이제 접근 방식의 근본적인 변화가 시급하다는 점을 인식하게 되기를 바랍니다.

개인 정보 보호법이 필요합니다.

44 Andrew Tutt, 알고리즘 FDA, 69 Admin. L. Rev. 83 (2017).

45 Frank H. Easterbrook, 사이버 공간과 말의 법칙, 1996 U. Chi. 법률 F. 207.

46 Alicia Solow-Niederman, 인공 지능 관리, 93 S. Cal. L. Rev. 633(2020)("AI의 역동적이고 교차적인 특성을 고려할 때" AI를 규제하는 단일 기관을 갖는 것이 어려울 것이라고 주장함).

II. AI 및 개인 정보 보호에 대한 규제 로드맵

AI의 심연을 탐구하면서 조심
스럽게 나아가고 우리가 놓칠 수 있
는 위험을 항상 인식하도록 합시다.

– 채팅GPT

이 부분에서는 AI와 개인 정보 보호에 대한 규제 로드맵을 제공하고 AI의 개인 정보 보호 문제를 해결하기 위해 개인 정보 보호법이 어떻게 변경되고 적응해야 하는지 논의합니다. 이 로드맵의 목표는 법이 해결해야 할 문제를 제기하고, 법의 이전 잘못된 접근 방식이 특히 AI에 부족한 이유를 지적하고, 법이 취해야 할 새로운 방향을 제안하는 것입니다. 나는 모델법을 제안하는 것이 아닙니다. 대신 이것은 로드맵과 가이드로서 더 광범위하고 개념적입니다.

AI는 오랫동안 지연된 개인 정보 보호법 변경이 필요한 이유를 보여줍니다.
결국 AI는 20세기 후반에 개인 정보 보호 문제를 제기하기 시작한 기술의 근본적으로 새로운 기술이 아닙니다. 오늘날의 차이점은 더 많은 데이터, 더 많은 컴퓨팅 성능, 더 나은 분석입니다.

AI의 개인 정보 보호 문제 중 상당수는 AI에 이미 존재했으며 AI에만 집중한다고 해서 해결될 수는 없습니다. 이를 처리하는 가장 좋은 방법은 뿌리에 집중하는 것입니다.
상단 가지를 잘라내는 것은 실제로 이러한 문제의 핵심을 해결하지 못합니다.
AI의 개인 정보 보호 문제는 기존의 개인 정보 보호 문제를 새로운 방식으로 결합하거나 새로운 수준으로 증폭시킨 것입니다. AI는 또한 기존 개인정보 보호법의 구별과 구조에 도전합니다. 이는 주의를 요하는 극명한 방식으로 이러한 법률의 균열, 공백 및 결함을 노출합니다.

이 부분은 디지털 시대의 개인 정보 보호 문제를 해결하는 데 오랫동안 부적합했던 이러한 법률의 기초인 개인 정보 보호 규제의 아키텍처와 접근 방식에 대한 광범위한 분석으로 시작됩니다. AI는 건물 전체를 붕괴시키겠다고 위협합니다. 쉬운 개조는 없습니다. 기초를 다시 세워야 합니다.

다음으로, 개인정보 보호법이 데이터 수집을 어떻게 규제해야 하는지 살펴보겠습니다. 데이터에 대한 AI의 끝없는 욕구는 데이터 수집에 대한 개인 정보 보호법의 규제에 심각한 도전을 제기합니다.
개인 정보 보호법의 일관되지 않은 개념과 접근 방식은 AI에 대한 많은 데이터가 수집되는 프로세스인 스크래핑을 해결하기에 부적절합니다. 합의된 데이터 수집에 대한 법적 접근 방식도 재검토되어야 합니다.

그런 다음 초점은 데이터 생성으로 전환됩니다. AI는 데이터를 생성하는 놀라운 능력을 제공하므로 많은 개인 정보 보호 문제를 악화시킵니다. AI는 예상하지 못한 개인에 대해 새로운 데이터가 생성되는 추론을 생성합니다.

결코 공유하고 싶지 않았습니다. 추론은 데이터 처리와 수집 사이의 경계를 모호하게 만들어 데이터 수집 제한과 많은 개인정보 보호법의 기타 보호를 회피할 수 있게 해줍니다. AI는 악의적인 물질도 생성할 수 있습니다.
사람과 사회에 심각한 해를 끼칠 수 있는 기만적이고 조작적인 콘텐츠입니다. 인간과 인간이 만든 콘텐츠를 시뮬레이션하는 AI의 능력은 속임수와 조작에 있어 새로운 차원을 열어줄 수 있습니다.

AI는 또한 사람에 대한 의사결정에 사용되어 개인정보 보호에 영향을 미칩니다. AI는 의사결정 방식을 바꿔 사람들의 치료와 기회에 영향을 미칠 수 있는 미래에 대한 예측을 촉진합니다. 이러한 예측은 인간의 선택 의지와 공정성에 대한 우려를 불러일으킵니다. AI는 사람에 대한 비예측적 결정에도 사용되어 편견이 이러한 결정에 영향을 미치는 방식을 변화시킵니다. AI 의사결정에는 자동화가 포함되기 때문에 지금까지 법이 해결하기 어려웠던 자동화된 프로세스로 인해 발생하는 문제가 있습니다.

AI는 또한 전례 없는 데이터 분석을 가능하게 하여 감시 및 식별을 크게 향상시킬 수 있습니다. 개인 정보 보호법은 오랫동안 감시 및 식별로 인해 발생하는 문제를 부적절하게 다루었습니다. AI는 이러한 문제를 새로운 차원으로 끌어올리고 골치 아픈 새로운 차원을 추가하겠다고 위협합니다.

마지막으로 이 부분에서는 개인정보 보호법이 AI에 대한 감독, 참여 및 책임을 어떻게 처리해야 하는지를 다룹니다. AI 기술이 작동하는 방식은 AI가 대부분 블랙박스로 작동하기 때문에 투명성과 같은 전통적인 감독 메커니즘을 복잡하게 만듭니다. AI는 적법한 프로세스 문제를 제시하여 개인이 AI의 결정과 효과에 이의를 제기하기 어렵게 만듭니다. AI 도구의 개발은 많은 이해관계자의 참여를 배제하는 경우가 많아 대표성이 떨어지고 다양성이 부족합니다. AI에 대한 책임성도 강화해야 하고, 개인정보 침해에 대한 효과적인 구제책도 필요하다.

A. 법적 구조 및 접근 방식

1. 개인의 통제와 자기관리를 넘어

개인 정보 보호법은 개인이 자신의 개인 정보를 관리할 수 있도록 함으로써 개인에게 권한을 부여하려는 개인 통제 모델이 지배해 왔으며, 이를 제가 통칭하여 "개인 정보 보호 자기 관리"라고 부르는 일련의 작업입니다.

미국에서는 많은 개인 정보 보호법이 "고지 및 선택 접근 방식"을 통해 개인의 통제를 촉진하는 것을 목표로 합니다.48 조직에서는 수집하는 데이터, 데이터 사용 및 전송 방법, 보호 방법에 대한 공지를 게시합니다. 사람들은 회사와의 거래를 거부하거나 중단할 수 있습니다. 사람들이 옵트아웃하지 않으면, 그들은 가정됩니다

47 Daniel J. Solove, 개인 정보 보호 자기 관리 및 동의 딜레마, 126 Harv. L. Rev. 1880, 1880 (2013).

48 ID 참조. 1883-84년; Charlotte A. Tschider, 의미 있는 선택: 동의의 역사와 동의 신화에 대한 대안, 22 NCJL & Tech. 617(2021).

동의한 것. 많은 미국 개인정보 보호법에서는 기업이 특정 용도에 대해 거부권을 제공하도록 규정하고 있습니다.49 일부 법률에서는 사람들이 특정 용도에 대해 명시적으로 동의(동의)하도록 요구합니다.50 Daniel Susser 교수는 통지 및 선택 접근 방식을 다음과 같이 설명합니다. 그들은 제공된 사용자 정보를 원합니다. (1) 사용자에게 그렇게 하겠다고 말하고 (2) 사용자가 계속 진행하기로 선택합니다."51

수십 년 동안 통지 및 선택 접근 방식은 수많은 전문가들로부터 비효율적이며 어떤 사람들에게는 완전히 우스꽝스럽다는 이유로 오랫동안 공격을 받아왔습니다.52 법학 교수인 Woodrow Hartzog와 Neil Richards가 설명한 것처럼, "'통지'는 종종 땅을 묻는 것 이상의 의미가 없습니다. 빽빽한 개인정보 보호 정책의 세부 사항에 데이터 관행이 있는 반면, '선택'은 타협할 수 없는 데이터 관행이 있는 서비스를 선택하거나 그대로 두는 옵션으로 선택하는 것을 의미합니다."53 문제는 누구도 그렇게 하지 않는다는 것입니다. 개인정보 보호정책을 읽습니다. 사람들이 그것을 읽으려고 하면 이해하려고 노력합니다. 각 회사의 개인 정보 보호 정책을 읽는 데는 무리한 시간이 소요됩니다. 그리고 그러한 통지가 사람들이 자신의 데이터 수집 및 사용에 대해 정보를 바탕으로 위험 결정을 내리는 데 도움이 되는지가 확실하지 않습니다.54

EU에서는 GDPR에도 개인 통제에 대한 강력한 핵심이 있습니다. 미국의 통지 및 선택 접근 방식과 달리 GDPR은 거부 동의를 거부합니다.
동의는 명시적이어야 하며, 이는 사람들이 동의해야 함을 의미합니다.55 GDPR은 개인에게 데이터에 대한 액세스, 수정 또는 삭제 권한은 물론 데이터 이동성에 대한 권리와 같은 다양한 권리를 제공하여 개인의 통제를 강화합니다. GDPR은 또한 데이터 보호 영향 평가 수행, 데이터 최소화 참여, 처리 활동 기록 유지, 데이터 보호 보장 요구 사항과 같은 여러 가지 의무를 조직에 부과합니다. 디자인과 기본값.57 그러나 법학 교수인 Ari Waldman이 지적한 것처럼, 이러한 임무는 종종 회사 내부에서 공허한 "기호"로 수행됩니다.

---

49 예를 들어 CAN-SPAM Act, 15 USC § 7704(a)(3)(원치 않는 상업 이메일 수신을 거부할 수 있는 권리 제공)을 참조하십시오. 전화 소비자 보호법, 47 USC § 227(텔레마케팅 전화를 거부할 수 있는 권리 제공).

50 예를 들어 아동 온라인 개인정보 보호법, 15 USC § 6502(b)(부모는 자녀의 데이터 수집 및 사용에 동의해야 함)를 참조하세요. 비디오 개인정보 보호법, 18 USC § 2710(b)(2)(B)(소비자 개인 데이터 공개에 동의).

51 Daniel Susser, 통지 및 동의 이후의 통지: 동의 프레임워크가 그렇지 않더라도 개인 정보 공개가 가치 있는 이유, J. Info. 정책 37, 41-42(2019).

52 Neil Richards 및 Woodrow Hartzog, 디지털 동의의 병리학, 96 Wash. UL Rev. 1461, 1463(2019); Richard Warner 및 Robert Sloan, 통지와 선택을 넘어서: 개인정보 보호, 규범 및 동의, 14 J. High Tech. L. 370(2014); Helen Nissenbaum, 온라인 개인 정보 보호에 대한 상황별 접근 방식, 140 Daedalus 32, 34(2011).

53 Woodrow Hartzog & Neil Richards, 개인정보 보호의 헌법적 순간과 데이터 보호의 한계, 61 BCL Rev. 1687, 1704(2020)

54 Solove, Murky Consent, 위 각주 X, at X.

55 GDPR 조항. 4.11(유효한 동의를 위해서는 "명확한 긍정 조치" 필요).

56 GDPR 제3장, 데이터 주체의 권리, 조항을 참조하세요 . 12-23.

57 GDPR 조항. 35(데이터 보호 영향 평가); 미술. 30(처리 활동 기록) 제25조(설계 및 기본에 따른 데이터 보호); 미술. 5(c)(데이터 최소화).

way.58 개인의 권리를 보호하기 위한 많은 의무가 존재합니다. GDPR은 개인의 통제를 넘어선 발전을 이루었지만 여전히 규제가 적용됩니다.
무게가 너무 많이 나갑니다.

부분적으로 GDPR의 영향으로 인해 미국 개인 정보 보호법은 액세스, 수정, 삭제할 권리는 물론 데이터 이동성에 대한 권리와 같은 권리로 다소 기본적인 통지 및 선택 접근 방식을 보완했습니다.59 여러 주에서는 특정 상황에서 자동화된 데이터 처리를 거부할 권리.60

개인 정보 보호법에 의해 제공되는 통제는 개인에게 자신의 개인 정보를 관리할 책임을 부여 하지만 개인은 이를 수행할 준비가 되어 있지 않습니다.61 명시적 동의가 통지 및 선택 접근 방식보다 훨씬 우수하지만 여전히 개인의 능력에 크게 의존합니다. 개인은 자신의 데이터 수집 및 사용에 관해 의미 있는 결정을 내릴 수 있습니다. 본질적으로 개인 정보 보호법은 개인에게 자신의 개인 정보를 관리할 책임을 위임하며, 이는 이익보다는 부담이 될 수 있습니다. 62 개인정보 보호 권리를 행사할 책임은 개인에게 있으며, 이는 자신의 데이터를 수집하고 사용하는 수천 개의 회사에서는 불가능하지는 않더라도 어려운 일입니다. 사람들은 각각의 데이터를 관리할 시간이 없습니다.63

더욱이, 사람들은 자신의 개인 데이터의 수집, 사용 또는 공개가 피해 위험을 초래할지 여부를 판단할 수 있는 전문 지식이 부족합니다. 오늘날의 AI 세계에서 자동화된 의사결정을 지원하는 알고리즘은 사람들이 이해하기에는 너무 복잡합니다. 이러한 알고리즘은 엄청난 양의 데이터에 의존합니다. 위험을 평가할 수 있으려면 사람들은 전문 데이터 과학자가 되어야 하며 알고리즘을 훈련하는 데 사용되는 데이터를 검토할 수도 있어야 하는데 이는 불가능합니다.64

법은 개인에게 진정으로 권한을 부여하기보다는 권한 부여의 외관을 만들어 아이러니하게도 더 많은 권한 박탈을 초래합니다. 이 상황
끝없이 달성할 수 없는 과제를 사람들에게 떠맡깁니다. 사람들이 예상대로 이 모든 일을 하지 않을 때, 그들은 자신의 프라이버시를 신경 쓰지 않는다는 비난을 받습니다.65

AI 알고리즘은 고립된 개별 데이터가 아닌 대규모 집단 데이터세트에서 작동합니다. Alicia Solow-Niederman이 말한 것처럼 현대의 "추론 경제"에서는

---

58 ARI EZRA WALDMAN, 자유로운 산업: 개인 정보 보호, 데이터 및 기업 권력 의 내부 이야기 115 (2021).

59 Va. Code Ann 참조 . § 59.1-575(2023); 콜로라도 목사 통계. § 6-1-1303(24)(2021); 유타 코드 앤. § 13-61-101(32)(2023); 2023 코네티컷 출판. 사도행전 22-15 § 1(27).

60 Liisa M. Thomas, 포괄적인 개인정보 보호법의 대홍수: "프로파일링"에 관해 해야 할 일, National L. Rev.(2023년 6월 26일).

61 Daniel J. Solove, 개인 정보 보호 권리의 제한, 98 Notre Dame L. Rev. 975, 993(2023).

62 Ella Corren, 소비자 및 디지털 시장의 동의 부담, 36 Harv. 제이엘앤테크. 551(2023).

63 Aleecia M. McDonald 및 Lorrie Faith Cranor, The Cost of Reading Privacy Policies, 4 I/S 540, 565(2008) 참조 (모든 개인 정보 보호 정책을 읽는 데는 연간 200시간 이상이 소요됩니다).

64 Solove, Murky Consent, 각주 X, 127-29.

65 Daniel J. Solove, 프라이버시 역설의 신화, 89 Geo. Wash. L. Rev. 1, 11-14 (2021).

기계 학습 및 알고리즘 의사 결정에 의해 주도되는 데이터의 역할은 근본적으로 집단적입니다.66 이러한 기술은 많은 사람에 대한 정보가 포함된 데이터 세트에서 추론을 이끌어 내는 방식으로 작동합니다. Salomé Viljoen이 지적했듯이 알고리즘은 개인 간의 유사성을 식별하여 생물학적, 대인 관계, 정치적, 경제적 연결에 대한 의미 있는 통찰력을 밝혀냅니다.67 Solow-Niederman과 Viljoen은 데이터의 관계형 특성을 강조합니다.

AI 알고리즘에는 일반적으로 수백만 명의 개인을 포함하는 대규모 데이터 세트 내에서 패턴을 식별하는 작업이 포함됩니다. 이러한 맥락에서 개인에게만 초점을 맞춘 권리와 보호는 부족합니다. 의사결정 방식이나 이러한 시스템 내에서 개인 데이터가 사용되는 방식을 이해하려는 개인은 그림의 일부만 파악할 수 있습니다. 이러한 알고리즘의 의사결정 과정을 완전히 이해하려면 알고리즘의 데이터 세트에 포함된 모든 개인의 집단 데이터를 고려해야 합니다. 하지만 이 데이터는 데이터세트에 포함된 사람들의 개인정보를 침해하지 않고는 개인에게 제공될 수 없습니다. 개인이 이 엄청난 양의 데이터를 분석하는 것도 불가능합니다.

개인 정보 보호 권리는 일반적으로 개인 기록의 정확성이나 데이터 수집에 대한 동의 여부 등 개인 수준의 문제에 집중하기 때문에 부족한 경우가 많습니다. 그러나 이러한 접근 방식은 시스템 문제를 해결하는 데 적합하지 않습니다. 예를 들어 공정신용보고법(FCRA)은 개인이 자신의 기록에 있는 오류를 수정할 수 있도록 허용하지만 신용 평가 시스템의 기본 원칙에 도전하지는 않습니다.68

개인은 자신의 데이터에 있는 실수를 바로잡을 수 있는 능력이 있지만 자신의 신용도를 판단하는 데 사용되는 방법론에 대한 영향력이나 의지가 부족합니다. 소비자 신고 기관이 액세스 및 수정 옵션을 제공하는 한 의사 결정 과정에서 상당한 권한을 유지합니다. 이는 이러한 회사가 사용하는 알고리즘에서 발생하는 잠재적인 불공정성과 문제를 간과하고 있습니다.69

AI의 등장으로 인해 개인 제어 모델이 종말을 고하게 되었다는 사실이 더욱 분명해졌습니다. AI는 개인이 개인 정보 보호에 미치는 영향을 이해하고 평가하기에는 너무 방대하고 복잡합니다. 개인에게 자신의 데이터에 대한 통제권을 부여하는 대신, 법은 데이터 수집 및 사용을 통제해야 합니다. 어떤 상황에서는 개인 정보 보호 권리가 도움이 될 수 있지만, 개인 정보 보호법은 이에 너무 과도하게 의존하는 것을 중단하고 개인에게 부담을 주지 않는 구조적 조치에 더 중점을 두어야 합니다. 효과적인 개인정보 보호는 현대 디지털 경제의 아키텍처에 초점을 맞춰야 합니다. 위험과 피해를 피하기 위해 조직에 의미 있는 의무를 부과해야 합니다. 그리고 그것은 유지되어야합니다

---

66 Alicia Solow-Niederman, 정보 프라이버시 및 추론 경제, 117 Nw. L. 개정 357, 361(2022).

67 Salomé Viljoen, 민주적 데이터: 데이터 거버넌스를 위한 관계형 이론, 131 Yale LJ 573, 578-79(2021).

68 공정 신용 보고법, 15 US Code § 1681. FCRA는 "최대한의 정확성을 보장하기 위한 합리적인 절차" § 1681e(b)를 요구하며 개인이 정확성에 대해 이의를 제기할 수 있도록 허용합니다. § 1681i(a)(1).
69 Solove, 개인정보 보호 권리의 제한, 각주 X, 1034.

조직은 의미 있는 방식으로 책임을 집니다.70

2. 피해 및 위험 분석

AI를 다루는 새로운 법률은 다른 접근 방식을 취하고 있습니다. 이러한 법률은 개인의 통제에 초점을 맞추는 대신 피해와 위험을 고려합니다. AI 법을 제정한 EU가 책임을 주도하고 있습니다.71 이 법은 (1) 허용할 수 없는 위험, (2) 높은 위험, (3) 제한된 위험이라는 세 가지 범주의 위험을 생성합니다. 허용할 수 없는 위험을 생성하는 AI 시스템은 금지됩니다. 다른 두 가지 위험 범주의 경우 제한 및 보호는 해당 범주에 비례합니다. 법학 교수인 Margot Kaminski가 지적했듯이 "위험 규제의 핵심 개념은 불확실성에 직면하여 규제 기관이 기술을 금지하거나 과도하게 규제해서는 안 되며 오히려 알려지고 측정 가능한 피해를 줄이는 데 노력을 기울여야 한다는 것입니다."72

피해와 위험에 초점을 맞추는 것은 올바른 방향으로 나아가는 단계이며, AI뿐만 아니라 개인 정보 보호법 전체가 해야 할 일입니다. 73 일부 개인정보 보호법은 어느 정도 피해와 위험에 중점을 두고 있습니다. 예를 들어, 많은 개인 정보 보호법에서는 특정 상황에서 위험 평가를 요구합니다. GDPR에는 조직이 "자연인의 권리와 자유에 대한 높은 위험"과 관련된 상황에서 데이터 보호 영향 평가(DPIA)를 수행해야 한다는 요구 사항이 있습니다.74

"권리와 자유"에는 "언론의 자유, 사상의 자유, 이동의 자유, 차별 금지, 자유, 양심 및 종교에 대한 권리"와 같은 사생활 보호와 기본권이 모두 포함됩니다. GDPR은 고위험의 세 가지 예를 나열합니다 . 처리 중 하나에는 "프로파일링을 포함하여 결정이 개인에게 법적 영향을 미치거나 이와 유사하게 중요한 영향을 미치는 체계적이고 광범위한 처리 활동"이 포함됩니다.76 GDPR에서 영감을 받은 많은 미국 주 소비자 개인 정보 보호법은 자동화된 의사 결정에 대한 위험 평가를 요구합니다. 또는 프로파일링.77

그러나 법이 해결해야 할 피해 및 위험 접근 방식에는 여전히 과제가 있습니다. Margot Kaminski는 위험 규제에 대한 우려를 제기합니다.

---

70 DANIEL J. SOLOVE, THE DIGITAL PER: TECHNOLOGY AND PRIVACY IN THE INFORMATION AGE 101 (2004) ("프라이버시 보호는 권력을 구조화하는 아키텍처, 정보가 전파되고 수집되는 방식을 통제하는 규제 프레임워크에 달려 있습니다. 네트워크로 연결되어 있어 권력 통제에 집중해야 합니다."); Dennis Hirsch, 개인 정보 보호법의 새로운 패러다임, 79 Md. L.
Rev. 439, 462 (2019) (개인 정보 보호에 대한 새로운 제안은 개인의 선택을 촉진하려는 자유주의적 규제 접근 방식에서 공무원이 선택할 수 있는 권한을 부여하는 접근 방식으로 전환하면서 "개인 통제보다는 사회적 보호"를 강조합니다. · · · 관행은 개인에게 안전하고 사회적 가치와 일치하지만 그렇지 않습니다.")

71 유럽 위원회, 인공 지능 – 질문과 답변 (2023년 12월 12일), https://ec.europa.eu/commission/presscorner/detail/en/QANDA_21_1683.

72 Margot E. Kaminski, AI 위험 규제, 103 BUL Rev. 1347(2023).

73 Daniel J. Solove, 데이터가 하는 일: 민감한 데이터 대신 사용, 피해 및 위험 규제, 118 Nw. UL 개정 1081, 1128-36(2024).

74 GDPR 조항. 5.

75 GDPR 조항. 5.

76 GDPR 조항. 5.

77 Liisa M. Thomas, 포괄적인 개인 정보 보호법 대홍수: "프로파일링"에 관해 해야 할 일, National L. Rev.(2023년 6월 26일).

프레임워크는 종종 “정량화할 수 없고 논쟁의 여지가 있는 개별화된 피해에 적합하지 않습니다.”78 비록 개인 제어 모델이 AI의 개인 정보 보호 문제를 해결하기에는 충분하지 않지만 AI는 여전히 개인에게 해를 끼치며 이러한 피해는 시정 가능해야 합니다. 개인 통제에 덜 의존한다고 해서 피해로부터 보호하지 못하는 것은 아닙니다. 피해 및 위험 접근 방식은 사회와 개인 모두에 대한 피해와 위험을 다루어야 하며 피해를 입은 개인에게 구제 메커니즘을 제공해야 합니다.

유해성 및 위험 접근 방식의 까다로운 문제는 누가 유해성 및 위험을 평가해야 하는지 결정하는 것입니다. 조직은 자체 AI 시스템의 피해와 위험을 평가할 책임이 있습니까? 아니면 정부 기관이 평가를 수행해야 합니까? 대부분의 법률은 조직에 의존하여 발생하는 위험을 평가하는데, 이는 여우에게 닭장에 있는 닭에 대한 위험을 평가하도록 요청하는 것과 유사할 수 있습니다.

조직이 평가를 수행하는 경우 어려운 문제는 법률이 평가를 규제 기관이나 대중과 공유하도록 요구해야 하는지 여부입니다. 대부분의 법률에는 그러한 요구 사항이 없습니다.79 조직 외부에 평가를 공개하면 조직이 더 책임감을 갖게 되어 피상적인 평가를 수행한 후 아무런 조치도 취하지 않게 됩니다. 반면에 위험 평가 공유를 요구하면 솔직함이 줄어들고 외부 홍보 활동으로 바뀔 수 있습니다.

또 다른 어려운 문제는 사용자가 무수히 다양한 방식으로 사용하는 생성 AI나 기타 AI 도구를 어떻게 처리할지입니다. 용도가 너무 많으면 잠재적인 피해와 위험이 많이 있을 수 있습니다. 나탈리 헬베르거와 니콜라스 디아코풀로스
생성적 AI 시스템은 특정 상황이나 사용 조건에 맞게 구축되지 않았으며 개방성과 제어 용이성은 전례 없는 규모의 사용을 가능하게 하기 때문에 생성적 AI의 위험 분석이 어려울 것이라고 주장합니다.80
Josephine Wolff, William Lehr, Christopher Yu는 "범용 AI가 제기하는 핵심 문제는 이와 관련된 위험을 의미 있는 방식으로 평가하는 것이 거의 불가능하다는 것"이라고 주장합니다.81 또한 그들은 "GDPR에 대해 다음과 같이 주장합니다 ." , 가장 큰 문제는 어떤 조치도 수행하는 것이 거의 불가능하다는 것입니다.
훈련에 사용되는 데이터에 대한 의미 있는 목적 제한(또는 데이터 최소화)
일반 AI 시스템.”82

또 다른 문제는 규제 검토 시기입니다. 규제 기관은 AI 기술을 배포하기 전에 검토해야 합니까? 그렇게 하면 위험할 정도로 가까워질 수 있습니다.

---

78 Kaminski, AI의 위험, 각주 X, at 1379.
79 주목할만한 예외에는 위험 평가를 규제 기관에 제출하도록 요구하는 CCPA, § 1798.185(a)(15)가 포함됩니다.

80 Natali Helberger 및 Nicholas Diakopoulos, ChatGPT 및 AI 법, 12 Internet Pol'y Rev. 1, 3(2023).

81 Josephine Wolff, William Lehr, Christopher Yu, AI 정책 수립을 위한 GDPR의 교훈,
27 버지니아 JL & 테크. 1, 22(2024).
82 ID.

규제 기관이 검토를 수행하는 동안 대기 기간으로 인해 혁신이 느려질 수 있는 라이선스 시스템으로 전환됩니다. 배포 후 AI 검토는 피해를 막기에는 너무 늦을 수 있습니다. 이러한 문제는 궁극적으로 유해성 및 위험 접근 방식을 검토하고 균형을 맞춰야 합니다.

B. 데이터 수집

AI는 전례 없는 양의 데이터 수집을 가져왔습니다. 83 AI를 위한 개인 데이터는 주로 인터넷에서 데이터를 스크랩하거나 고객 또는 사용자 데이터의 용도를 변경하는 두 가지 방법으로 수집됩니다. 데이터에 대한 AI의 갈증은 데이터 수집에 대한 의미 있는 통제를 시도하는 개인 정보 보호법에 엄청난 스트레스를 가하고 있습니다. 많은 경우에. AI는 많은 개인 정보 보호법의 보호를 피할 수 있습니다. 다른 상황에서는 일부 법률이 엄격하게 해석되고 시행될 경우 AI에 대한 데이터 수집을 크게 제한하여 AI 기능에 필요한 데이터가 부족해질 수 있습니다. 데이터 공급 열풍과 데이터 기근 사이의 중간 지점을 찾는 것은 어려울 것입니다.

1. 긁기

기계 학습 알고리즘은 훈련을 위해 광범위한 데이터를 필요로 하며, 인터넷은 가장 접근하기 쉬운 공급처입니다. 예를 들어, Clearview AI라는 회사는 소셜 미디어, 온라인 프로필, 사진 웹사이트에서 스크랩한 수십억 장의 사진을 수집하여 최고의 얼굴 인식 도구 중 하나를 개발했습니다. 회사는 개인이 결코 예상하지 못한 이미지를 사용하여 동의를 구하지 않고 이를 수행했습니다. 이는 법 집행 및 정부 감시를 위한 방대한 AI 네트워크의 일부가 될 것입니다.84 많은 기업이 유사한 데이터 스크랩 관행에 참여하고 있습니다. 다양한 조직이 AI 시스템의 끝없는 요구 사항을 충족하기 위해 끊임없이 온라인 데이터를 추출합니다.85

(a) 스크래핑 및 개인정보 보호 원칙

웹 스크래핑은 법률, 업계 규정 또는 승인된 표준에서 일반적으로 인정되는 많은 개인 정보 보호 원칙을 위반합니다. 이러한 원칙에는 개인 데이터 수집 및 사용에 대한 투명성이 포함됩니다. 개인에게 개인정보 보호정책을 알리는 것 개인 데이터 사용 목적을 정의합니다. 관련 없는 2차 목적으로 데이터를 사용하는 것을 방지합니다. 데이터 사용에 대한 동의를 구하거나 거부 옵션을 제공합니다. 제3자 데이터에 대한 정보 제공

---

83 Charlotte A. Tschider, AI의 정당한 이익: 공익 프라이버시 모델을 향하여 21 Hous. J. Health L. & Policy 125, 132(2021)("기계 학습 애플리케이션은 예외적으로 많은 양의 데이터를 사용하며, 이러한 데이터는 기계 학습 유틸리티로 분석되어 이러한 데이터 간의 상호 관계를 결정합니다.")

84 카슈미르 힐, 당신의 얼굴은 우리 의 것입니다 ; 우리가 알고 있는 개인 정보 보호를 종식시키기 위한 비밀스러운 스타트업의 탐구 (2023).

85 Kieran McCarthy, "나를 위한 웹 스크래핑이지만 당신을 위한 것은 아닙니다." Tech. & Marketing L. 블로그 (2023년 8월 24일)(ChatGPT가 "거의 확실히 인증되지 않은 인터넷 전체를 이미 스크랩하고" ChatGPT를 교육하는 데 데이터를 사용했다는 내용은 없습니다), https://blog.ericgoldman.org/아카이브/2023/08/web-scraping-for-me-but-not-for-thee-guest-blog-post.htm.

수신자; 제3자에게 데이터를 전송하기 전에 실사를 수행합니다. 데이터 보호를 보장하기 위해 개인 데이터의 제3자 수신자와 계약을 체결합니다. 접근, 수정, 삭제, 이동성을 포함하여 개인 데이터에 대한 권리를 개인에게 부여합니다. 명시된 목적에 필요한 기간 동안만 데이터를 보관합니다. 데이터를 적절하게 폐기합니다. 유지

데이터 정확성; 무단 데이터 액세스로부터 보호합니다.86 스크래핑은 본질적으로 이러한 모든 원칙을 무시합니다. 데이터는 통지, 동의, 심사, 보호 장치, 지정된 목적, 목적 제한, 데이터 최소화, 개인 권리, 보존 제한 등 없이 제3자 스크레이퍼에 의해 가져가게 됩니다. 기본적으로 스크래핑에는 개인 정보 보호 고려 사항이 없습니다.

스크래핑은 기계 학습 알고리즘이 대중화되고 널리 사용되기 훨씬 전에 발생했습니다. 따라서 스크래핑은 AI에만 국한된 문제가 아닙니다. 그러나 AI는 스크레이핑을 더 자주, 광범위하게 수행할 인센티브를 생성하기 때문에 스크래핑을 극적으로 확대합니다.

(b) 공개적으로 이용 가능한 데이터

미국에서는 스크래핑이 온라인에서 공개적으로 접근할 수 있는 데이터를 표적으로 삼기 때문에 지금까지 개인정보 보호법에 대한 중요한 개입을 피했습니다. 스크레이핑을 하는 사람들은 공개적으로 이용 가능한 데이터에 개인 정보 보호 문제가 적용되지 않는다는 가정 하에 활동하며, 자유롭게 접근할 수 있다고 믿는 경우가 많습니다.

많은 개인 정보 보호법은 개인 정보가 숨겨져 있는 경우에만 개인 데이터를 비공개로 간주하는 단순한 이진법 개념을 채택합니다. 저는 이 개념을 "비밀 패러다임"이라고 부릅니다. 87
그러나 개인정보 보호는 훨씬 더 복잡합니다. 이는 데이터가 공유되는 방식을 모듈화하는 일련의 경계를 수반합니다.88 개인이 자신의 데이터를 완전히 비공개로 유지하는 경우는 거의 없습니다.
보다 일반적으로 그들은 친구, 가족, 직장 동료 또는 유사한 건강 문제에 직면하거나 동일한 중독과 싸우는 사람들과 같이 공통 관심사를 가진 그룹 구성원과 같은 특정 사회적 범위 내에서 이를 공개합니다.

여러 학자들이 설득력 있게 주장했듯이, 사람들은 공공장소에서 어느 정도의 프라이버시를 기대하며, 그러한 기대는 합리적일 뿐만 아니라 자유, 민주주의, 개인의 행복을 위해 중요합니다. 89 일상생활에서 우리는

---

86 GDPR, CCPA 등 일부 개인정보 보호법에만 이러한 원칙이 모두 포함되어 있지만, 많은 개인정보 보호법에는 이러한 원칙의 대부분이 포함되어 있습니다. 또한 이러한 원칙 중 다수는 1980년 경제협력개발기구(OECD) 지침과 같은 영향력 있는 체계에서 발견됩니다. NIST(국립표준기술연구소) 개인정보 보호 프레임워크 (2020년 1월 6일), https://www.nist.gov/privacy-framework; 및 AMERICAN LA INSTITUTE의 법률 원칙 , 데이터 개인정보 보호 (2019년 5월 22일).

87 DANIEL J. SOLOVE, 디지털 인물: 정보 시대 의 기술과 개인 정보 보호 (2004).

88 Lior Jacob Strahilevitz, 개인 정보 보호에 대한 소셜 네트워크 이론, 72 시카고 대학교 법률 검토 919(2005).
89 Helen Nissenbaum, 정보화 시대의 개인 정보 보호: 공공의 개인 정보 보호 문제, 17 Law & Phil. 559(1998); Helen Nissenbaum, 공공의 개인 정보 보호에 대한 접근 방식: 정보 기술의 과제, 7 윤리 및 행동. 207, 208(1997); Joel R. Reidenberg, 공개 프라이버시, 69 U. Miami L. Rev. 141, 157-59 (2014); Woodrow Hartzog, 공공 정보 오류, 99 BUL Rev. 459, 522(2019).

데이터는 실질적으로 모호하게 보호됩니다.90 데이터가 대중에게 노출될 수 있더라도 찾기 어렵고 일반적으로 관찰 또는 기록되지 않으며 단편화되고 널리 분산되어 있기 때문에 데이터에는 여전히 개인 정보 보호 이익이 있을 수 있습니다.
더욱이, 지적재산권법이 보여주듯이, 공개적으로 이용 가능한 정보라도 법이 강력한 보호를 제공하는 것이 가능합니다.91 개인 정보 보호법은 이름이나 초상 도용 불법 행위와 같이 특정 상황에도 불구하고 보호를 제공하는 경우에도 이를 수행합니다. 이 데이터의 공개 가용성.92

AI 시대에 개인정보 보호가 진정으로 효과적이려면 법이 단순한 이분법적 관점을 넘어 모호함을 보호해야 합니다. 93
조직은 적합하다고 판단되는 어떤 목적으로든 인터넷에서 개인 데이터를 무차별적으로 수집할 수 없어야 합니다.

공개적으로 이용 가능한 데이터에 대한 개인정보 보호법의 입장은 현재 일관성이 없습니다. EU의 일반 데이터 보호 규정과 같은 일부 법률은 대부분의 상황에서 공개적으로 이용 가능한 데이터를 면제하지 않지만 다른 법률에서는 면제합니다.94 예를 들어 캘리포니아 소비자 개인 정보 보호법(CCPA)은 다음의 데이터를 포함하는 "공개적으로 이용 가능한 정보"를 면제합니다. 정부 기록 및 널리 배포된 매체에 게시되거나 데이터 주체 또는 데이터 주체가 데이터를 특정 대상으로 제한하지 않은 다른 사람에 의해 일반 대중에게 제공되는 데이터.95 유타 및 버지니아와 같은 기타 주, 소비자 개인정보 보호법에서도 유사한 면제 조항을 두고 있습니다.96 그러나 일부 주에서는 "공개적으로 이용 가능한 정보"를 면제하기는 하지만 용어에 대한 정의가 훨씬 더 좁습니다. 예를 들어, 콜로라도에는 정부 기록의 데이터와 데이터 주체가 일반 대중에게 제공한 데이터만 포함됩니다.97 코네티컷에는 콜로라도와 동일한 범주가 포함되지만 미디어에 의해 전파되는 데이터도 포함됩니다.98 예를 들어 개인 정보 보호 변호사 David Zetoony가 관찰한 것처럼 , "일부 기업에서는 인터넷에서 사용할 수 있는 정보를 '공개적으로 사용할 수 있는 정보'로 간주할 수 있지만 대부분의 데이터 개인정보 보호법은 인터넷에서 액세스할 수 있는 모든 정보를 '공개적으로 사용할 수 있는 정보'로 분류하지 않습니다."99

---

90 Woodrow Hartzog & Evan Selinger, 모호함의 상실로서의 감시, 72 Wash. & Lee L. Rev. 1343, 1349 (2015).

91 다니엘 J. 솔러브(DANIEL J. SOLOVE), 평판 의 미래 : 인터넷 상의 가십 , 소문, 개인 정보 보호 184-86(2007).

92 불법 행위에 대한 재진술(두 번째) § 652C.

93 Woodrow Hartzog & Frederic Stutzman, 디자인에 의한 모호함, 88 Wash. L. Rev. 385, 407 (2013). 나는 "접근성 향상"이라는 용어를 사용하여 모호함의 문제를 논의했습니다. 사랑해요, 개인정보 보호 에 대한 이해 , 위의 94 GDPR
은 일반적으로 공개적으로 이용 가능한 데이터로부터 보호하지만 "데이터 주체가 명백히 공개한 개인 데이터"는 제외합니다. GDPR 예술. 9.2(e).

95 칼로리 문명 규정 § 1798.140(v)(2)(West 2021).

96 버지니아주법 § 59.1-571(2021); 유타 코드 앤. § 13-61-101(29)(b)(2022).

97 CRS § 6-1-1303(17)(b)(2021).

98 코네티컷 데이터 개인 정보 보호법, § 1(25).

99 David Zetoony, 주 개인정보 보호법에 따라 '공개적으로 이용 가능한 정보'란 무엇입니까? 국내법 검토(2023년 9월 13일) https://www.natlawreview.com/article/what-publicly-

일부 미국 연방법은 공개적으로 이용 가능한 데이터를 제외하지 않습니다. 예를 들어, 신용 보고를 규제하는 FCRA(Fair Credit Reporting Act)는 출처가 공개인지 비공개인지에 관계없이 소비자 보고 기관이 수집하고 사용하는 모든 데이터를 보호합니다. 신용 보고에 사용되는 데이터의 대부분은 재산, 면허, 형사 유죄 판결, 민사 판결, 파산 등과 같은 공공 기록에서 얻습니다. HIPAA는 공개적으로 이용 가능한 건강 데이터라도 보호합니다.100

많은 경우, 플랫폼의 개인 데이터는 무료로 제공되지 않지만 플랫폼의 서비스 약관에 따라 사용이 제한됩니다. 본 서비스 약관은 단순한 제안이 아닙니다. 그것은 용어입니다. LinkedIn에는 사용자가 사용자 프로필을 스크랩하기 위해 소프트웨어, 봇 또는 프로세스를 사용하지 않도록 요구하는 사용자 계약이 있습니다.101

더욱이, 미국 대법원의 Carpenter 대 United States 사건 , DOJ 대 언론자유기자위원회 사건과 같은 법적 판례에서는 공개 가용성이 개인의 개인정보 보호 권리를 부정하지 않는다는 점을 인정했습니다. Carpenter 사건에서 법원은 공공 차량 이동에 대한 지리적 위치 데이터를 수집하는 것이 합리적인 개인 정보 보호 기대치를 위반한다고 판결했습니다. 법원의 결정은 개인 정보 보호에 대한 접근 방식에 중요한 변화를 가져왔습니다. 이전에 법원은 공공 장소에서 관찰할 수 있는 모든 것은 사적인 것이 아니라고 주장했습니다.102 그러나 Carpenter 사건 에서 법원은 지리 위치 데이터가 공공 장소에서의 움직임을 자주 추적함에도 불구하고 "개인의 삶에 대한 친밀한 창"을 열어준다는 점을 인정했습니다. 103 법원은 GPS 데이터에 개인정보 보호에 대한 합리적인 기대가 있으며, 수정헌법 제4조의 보호를 보장하고 법집행기관이 해당 데이터에 접근하려면 수색 영장을 받아야 한다고 결정했습니다.

기자 위원회 에서 법원은 공개 기록의 개인 데이터가 여전히 개인 정보 보호 이익을 유지한다는 점을 인정했습니다. 한 언론 기관은 개인정보 보호 면제가 포함된 정보자유법에 따른 공개 정보라고 주장하면서 개인에 대한 FBI 서류에 접근하려고 했습니다. 언론은 이 정보가 다양한 공개 기록에서 나온 것이기 때문에 비공개가 아니라고 주장했습니다. 그러나 법원은 이에 동의하지 않았습니다. “전국의 법원 파일, 카운티 기록 보관소, 지방 경찰서를 부지런히 검색한 후 발견할 수 있는 공개 기록과 단일 정보센터에 있는 전산화된 요약 사이에는 분명히 큰 차이가 있습니다. 정보의.”104

주 개인정보 보호법에 따라 이용 가능한 정보.

100 HIPAA는 그것이 보호하는 건강 데이터가 공개적으로 이용 가능한 경우 면제를 포함하지 않습니다.

101 LinkedIn, 사용자 계약 8.2, https://www.linkedin.com/legal/user-agreement.

102 United States v. Knotts, 460 US 276 (1983) (공공 장소에서 장치를 추적하여 움직임을 모니터링할 때 개인 정보 보호에 대한 합리적인 기대가 없음); Florida v. Riley, 488 US 445(1989) (법적 공역을 비행하는 헬리콥터에 탑승한 경찰관이 자신의 사유지에서 볼 수 있는 모든 것에 대해 프라이버시를 기대하지 않음).

103 Carpenter v. United States, 138 S. Ct. 2206(2018).

104 미국 법무부 대 언론자유 기자위원회, 489 US 749(1989).

따라서 미국 개인 정보 보호법은 공개 노출 또는 공개 접근성이 더 이상 데이터에 대한 개인 정보 보호 관심이 없음을 의미하는지 여부에 대해 일관성이 없습니다. 개인 정보 보호가 효과적이려면 법적 프레임워크가 이진 정의를 넘어 모호함을 보호해야 합니다.

관련 문제는 플랫폼과 기타 조직이 데이터 스크랩을 방지해야 하는 의무와 관련이 있습니다. 개인 정보 보호법은 일반적으로 사이트가 스크래핑을 방지하도록 요구하지 않습니다. 서비스 약관에 따라 사용자 데이터를 보호한 다음 서비스 약관을 시행하는 것은 조직의 몫입니다. 그러나 개인 정보 보호법은 스크래핑에 대한 보호를 의무화해야 합니다. 조직이 동의 없이 대량의 개인 데이터를 제3자에게 전송하려고 시도하는 경우 이러한 관행은 많은 개인 정보 보호법을 위반하게 됩니다. 제3자가 데이터를 가져가는 것을 막지 못하는 것은 데이터를 판매하거나 공유하는 것과 기능적으로 동일합니다.

(c) 책임 있는 공공 기록

AI 시스템이 온라인 기록에서 개인 데이터를 무분별하게 수집하고 사용하는 데서 나타나는 문제를 고려할 때, 정부가 일상적으로 대중에게 배포하는 개인 데이터에 대해 최종적으로 책임 있는 통제를 행사하는 것이 필수적입니다.

원래 공개 기록법은 정부 운영의 투명성을 높이기 위해 제정되었습니다. 그러나 오늘날 공공 기록은 빅데이터 회사에서 개인 데이터를 수집하고 조합하는 데 주로 활용됩니다.

사람들이 정부에 대해 조명할 수 있도록 권한을 부여하기 위한 법률은 오히려 사람들에게 빛을 비추고 있습니다.105 공공 기록은 AI를 위한 무제한의 무료 데이터 원천이 되어서는 안 됩니다.

Los Angeles Police Department v. United Reporting Publishing Co. 의 경우 , 법령에 따라 체포된 공개 정보에 대한 접근이 제한되었으며, 신고자는 위증 시 처벌을 받는다는 조건 하에 해당 데이터가 "제품이나 서비스를 판매하기 위해 직간접적으로 사용되지 않을 것"임을 확인해야 했습니다. .” 이 동상은 상업적 표현을 침해한다는 이유로 이의를 제기 받았습니다. 그러나 미국 대법원은 이 법령을 표현 제한으로 간주하지 않았습니다. 오히려 이 법령은 "발언자가 이미 보유하고 있는 정보를 전달하는 것을 금지"하는 것이 아니라 단순히 "발표자가 보유하고 있는 정보에 대한 정부의 접근을 거부"하는 것입니다.106

이는 회사가 서비스 약관에 조건을 제공하는 방법과 유사하게 정부가 대중에게 공개하는 많은 데이터에 조건을 부여할 수 있다는 의미입니다. 정부는 특정 정보가 특정 방식으로 사용되지 않는다는 조건 하에 공개 기록을 공개할 수 있습니다. 이러한 구별은 실질적인 균형을 이룹니다. 조건부 액세스를 통해 대중은 광범위한 정보에 액세스할 수 있습니다.

---

105 Daniel J. Solove, 접근 및 집계: 공공 기록, 개인 정보 보호 및 헌법, 86 Minn. L. Rev. 1137, 1176-78(2002).

106 528 미국 32(1999).

개인 정보를 보호하는 동시에 기록의 배열.

수정헌법 제1조에 따라 허용되는 것 외에도 공공 기록에 있는 개인 데이터에 대한 접근 조건은 법에 따라 정부의 의무가 되어야 합니다. 법은 정부 기관이 개인 데이터에 대한 접근에 대해 합당한 조건을 마련하도록 요구해야 합니다. 어떠한 보호도 없이 개인정보를 인터넷에 방치하는 정부기관은 무책임하게 행동하고 있습니다.

2. "합의에 따른" 데이터 수집

(a) 동의의 허구

기업들은 AI 개발을 위해 사람들의 데이터를 사용할 것임을 나타내기 위해 개인 정보 보호 정책을 변경하기 시작했습니다. 예를 들어, 2023년 Zoom은 사용자가 Zoom의 "어떤 목적으로든 서비스 생성 데이터의 액세스, 사용, 수집, 생성, 수정, 배포, 처리, 공유, 유지 관리 및 저장"에 동의한다는 내용으로 개인 정보 보호 정책을 변경했습니다. 통지문에는 "모든 목적"에는 AI 알고리즘 훈련이 포함된다고 명시되어 있습니다. 또한 Zoom에는 사용자가 AI 교육 및 기타 목적으로 콘텐츠를 사용할 수 있는 "영구적이고 전 세계적이며 비독점적이고 로열티가 없는" 라이선스를 Zoom에 부여하는 조항도 포함되어 있습니다. 그러나 Zoom의 변화는 대중의 관심을 끌었고 회사는 뒤로 물러섰습니다.107

같은 해, 구글과 다른 회사들은 AI 수집을 제공하기 위해 개인정보 취급방침을 변경했습니다. Google은 "공개적으로 이용 가능한 정보를 사용하여 Google의 AI 모델을 교육하고 Google 번역, Bard 및 Cloud AI 기능과 같은 제품 및 기능을 구축하는 데 도움을 줍니다"라고 밝혔습니다. 이전에 Twitter였던 108 X는 개인 정보 보호 정책을 다음과 같이 변경했습니다. "우리는 이 정책에 설명된 목적을 위해 기계 학습 또는 인공 지능 모델을 훈련하는 데 도움을 주기 위해 수집한 정보와 공개적으로 사용 가능한 정보를 사용할 수 있습니다." 109

개인 정보 보호 정책을 변경하고 새로운 목적으로 개인 데이터를 수집 및 사용하는 관행은 AI에만 국한된 것이 아니라 일반적인 관행입니다. 많은 미국 개인 정보 보호법에서는 통지 및 선택 접근 방식에 따라 이러한 관행이 일반적으로 허용됩니다.110

EU의 GDPR은 통지 및 선택 접근 방식을 거부하고 대신

---

107 Ian Krietzberg, "Zoom Walks Back 논란의 여지가 있는 개인 정보 보호 정책", The Street(2023년 8월 11일).

108 Matthew G. Southern, "Google은 AI 훈련을 위한 공개 데이터를 수집하기 위해 개인정보 보호정책을 업데이트합니다." 검색 엔진 저널(2023년 7월 3일), https://www.searchenginejournal.com/google-updates-privacy-policy-to-collect-public-data-for-ai-training/490715/.

109 Sarah Perez, "X의 개인 정보 보호 정책은 AI 모델 교육에 공개 데이터를 사용할 것임을 확인합니다." Tech Crunch(2023년 9월 1일).

110 미국 개인 정보 보호법의 통지 및 선택 접근 방식의 예로는 CAN-SPAM법, 15 USC § 7704(a)(3)(사람들이 거부하지 않는 한 회사가 원치 않는 상업 이메일을 사람들에게 보낼 수 있도록 허용), 전화 소비자 보호법, 47 USC § 227(사람들이 거부하지 않는 한 텔레마케터가 사람들에게 전화할 수 있도록 허용).

명시적인 동의(동의)가 필요하지만111 이러한 강력한 형태의 동의도 의미가 없습니다. 동의를 하려면 수락 버튼만 클릭하면 되는 경우가 많습니다. 이는 사람들이 개인 정보 보호 정책을 읽었거나 관련된 위험을 이해했다는 것을 보장하지 않습니다. 사람들에게 동의 버튼이나 상자를 통해 명시적인 동의를 표시하도록 강요하더라도 알림의 독자층이 거의 증가하지 않습니다.112 다른 연구에서 나는 동의가 옵트 아웃이든 옵트 인이든 상관없이 여전히 대부분의 경우 동의한다는 점을 주장했습니다. 허구.113

AI는 방정식을 더욱 복잡하게 만듭니다. 그것은 소설을 더욱 환상적으로 만든다. 예를 들어 생성 AI의 경우 구체적인 용도가 알려지지 않은 경우가 많습니다. 생성적 AI 도구 사용자는 이를 무수히 다양한 용도로 사용할 수 있습니다. 일부는 양성이고 일부는 악성입니다. 동의는 거의 모든 일에 대한 백지 수표가 됩니다. AI를 사용하면 사람들은 자신이 무엇에 동의하는지 모르는 경우가 많습니다.

AI는 동의에 대한 접근 방식의 단점을 증폭시키지만 개인 정보 보호법은 오랫동안 동의에 너무 많이 의존하여 결함이 있었습니다. 동의 여부, 미국 개인 정보 보호법이나 GDPR 또는 전 세계의 많은 개인 정보 보호법에 따라 동의는 Elettra Bietti 교수가 적절하게 부르는 "자유 이용권"을 기업에 제공하여 엄청난 수의 방법으로 데이터를 사용할 수 있는 경우가 너무 많습니다. 114

(b) AI 데이터 수집 제한

반면, 동의 요구 사항은 상당한 이점이 있는 경우에도 AI 모델에 대한 개인 데이터 수집을 방해할 수 있습니다. 또한 스크래핑은 연구원과 언론인에게 도움이 될 수 있습니다. 기술 저널리스트 Julia Angwin은 저널리스트가 "폭군, 트롤, 스파이, 마케터 및 증오 군중이 어떻게 기술 플랫폼을 무기화하거나 이를 통해 활성화되는지" 조사하려면 "대량의 공개 데이터에 접근할 수 있어야 합니다."라고 지적합니다. . 사건이 변칙적인 것인지 아니면 더 큰 추세를 나타내는 것인지 이해하는 것입니다."115 인터넷을 통해 AI 데이터를 수집하는 경우 명시적인 개인 동의를 얻는 것은 불가능하지는 않더라도 어려운 과제입니다.

GDPR에는 공개적으로 이용 가능한 정보에 대한 예외가 포함되어 있지 않습니다. 조직이 GDPR에 따라 데이터를 수집할 수 있는 유일한 방법은 데이터 주체에 대한 데이터를 수집하기 위한 6가지 법적 근거 중 하나를 갖는 것입니다. (1) 동의; (2) 계약에 필요한 경우; (3) 법적 의무를 준수하는 데 필요한 경우 (4) 개인의 중요한 이익을 보호하는 데 필요한 경우 (5) 공익을 위해 필요한 경우; 그리고 (6)

---

111 GDPR, 예술. 4(11) ("자유롭게 제공되고, 구체적이고, 정보에 입각하고, 모호하지 않게 동의해야 함) 정보주체의 희망사항 표시").

112 Florencia Marotta-Wurgler, 공개 증가가 도움이 될까요? ALI의 "소프트웨어 계약법 원칙"에 대한 권장 사항 평가, 78 U. Chi. L. Rev. 165, 168(2011)(사람들이 용어 옆에 있는 "동의함" 상자를 클릭하도록 요구하면 독자층이 1%만 증가했음을 보여주는 연구).

113 Solove, Murky Consent, 위 각주 X, at X.

114 Elettra Bietti, 프리 패스로서의 동의: 플랫폼 전력 및 정보 전환의 한계, 40 Pace L. Rev. 308, 313(2020).

115 Julia Angwin, "지식의 문지기는 그들이 아는 것을 우리가 보기를 원하지 않습니다." NY 타임즈(2023년 7월 14일).

합법적인 이익을 위해 필요하며 "정보 주체의 이익이나 기본적 권리 및 자유에 의해 무시"되지 않습니다. 116

GDPR에 따라 대기업은 수백만 또는 수십억 명의 사용자로부터 동의를 얻을 수 있는 방법을 찾을 수 있습니다. 그러나 대규모 사용자 기반이 없는 소규모 회사는 자신이 통제할 수 없고 동의를 얻을 수 없는 소스에서 데이터를 수집해야 합니다. 이러한 소규모 회사는 AI 모델을 훈련하는 데 필요한 데이터의 양이 부족합니다.

HiQ Labs v. LinkedIn 에서 LinkedIn은 HiQ가 사용자 프로필에서 개인 데이터를 스크랩하는 것을 차단했습니다. HiQ는 이러한 차단이 반경쟁적이라고 주장했고 법원은 이에 동의했습니다.117 추가 소송이 계속되었고 사건은 최종적으로 해결되었습니다.
기업이 경쟁이라는 명목으로 개인정보 보호를 과시하도록 허용한 법원의 판단은 틀렸지만, 기업이 보유한 데이터만 사용할 수 있다면 대기업이 AI 개발에서 엄청난 이점을 갖게 될 것이라는 우려는 확실히 타당합니다.

GDPR에 따르면 가장 그럴듯한 법적 근거는 합법적인 이익입니다.118
그러나 GDPR은 적법한 이익에 대해 제한적이므로 AI의 특정 용도에 따라 이러한 기반의 사용이 어렵고 전혀 보장되지 않습니다.

GDPR이 EU에서 AI 데이터 수집을 광범위하게 제한하거나 특정 관할권의 개인 정보 보호법이 데이터 수집을 금지하는 경우 왜곡 효과가 발생할 수 있습니다. 예를 들어 EU나 특정 국가 출신의 사람들에 대한 훈련 데이터가 제외된다면 AI 모델은 데이터를 더 자유롭게 수집할 수 있는 곳의 사람들을 반영하는 쪽으로 치우칠 수 있습니다. AI 알고리즘은 데이터를 훈련받은 사람들의 문화적 관행과 행동을 강조합니다.

C. 데이터 생성

1. 추론

AI는 사람에 대해 추론하여 개인 정보 보호에 영향을 미칩니다. 추론은 내가 "집계 효과"라고 부르는 현상을 통해 발생합니다. 즉, 수많은 작은 개인 데이터를 수집하면 개인의 기여가 암시하는 것보다 훨씬 더 많은 것을 밝혀낼 수 있다는 사실입니다.119 현대 컴퓨팅의 발전으로 데이터의 기본 패턴을 탐지하는 능력이 크게 증폭되었습니다. AI 알고리즘은

116 GDPR 조항. 6.

117 HiQ Labs, Inc. v. LinkedIn Corp., 938 F.3d 985(2019년 9차). 개인정보 보호법과 반경쟁법 간의 충돌에 대한 배경 정보는 Erika M. Douglas, The New Antitrust/Data Privacy Law Interface, Yale LJ Forum(2021년 1월 18일)을 참조하세요.

118 Magali Feys, Herlad Jongen, Gary LaFever, AI에 대한 법적 근거 요구 사항, LinkedIn(7월 2023년 17월 17일), https://www.linkedin.com/pulse/legal-basis-requirements-ai-gary-lafever/.

119 SOLOVE, THE DIGITAL PERSON, 각주 X, 44-47.

개인에 대한 새로운 통찰력을 쉽게 추론할 수 있습니다.

Alicia Solow-Niederman이 지적했듯이 AI 알고리즘은 사람들이 기대하지 않는 방식으로 사람에 대한 새로운 데이터를 생성합니다. "기계 학습은 조직이 개인으로부터 수집한 사용 가능한 데이터를 사용하여 두 사람에 대한 추가 정보를 생성하는 추론 경제를 촉진합니다 . 개인과 다른 사람들에 관한 것입니다." 120 예를 들어, 사람들은 자신이 무해한 데이터를 공개하고 있다고 생각할 수 있지만 이 데이터는 건강, 종교, 정치적 신념, 성생활 및 기타 매우 개인적인 문제에 대한 민감한 정보를 추론하는 데 사용될 수 있습니다.121 Solow-Niederman이 지적한 것처럼 사람들은 (불가능하지는 않더라도) "어떤 데이터 비트가 중요한지 예측하는 것이 어렵습니다. 이 결과는 자신의 개인 데이터를 보호하려고 하지만 보호해야 할 항목이 무엇인지 더 이상 알 수 없는 개인의 역량을 약화시킵니다." 122

(a) 데이터 생성의 문제

개인정보 보호법은 개인에게 수집된 데이터에 대한 통지를 제공하지만, 생성된 데이터에 대한 통지는 제공하지 않는 경우가 많습니다 .
개인의 입장에서는 데이터가 수집되었는지 생성되었는지는 중요하지 않습니다. 궁극적인 결과는 그들이 기대하지도 않았고 동의하지도 않았던 그들에 관한 데이터가 알려지게 된다는 것입니다. 추론을 하면 생성된 데이터에서 사람들이 공개하고 싶어하지 않는 세부 정보가 드러날 때 심각한 개인 정보 침해가 발생할 수 있습니다. 이는 대형 소매점 체인인 Target과 관련된 잘 알려진 사건에서 강조되었습니다.

Target은 쇼핑 패턴을 기반으로 임산부를 식별하는 알고리즘을 개발했습니다. 목표는 임신을 조기에 인식하고 이러한 여성들이 Target을 유아용품 소매업체로 여기도록 장려하는 것이었습니다. 주목할 만한 사례로, 한 남성이 자신의 10대 딸이 수많은 아기 관련 광고를 받았다고 Target에 불만을 토로했습니다. 광고가 잘못 전송되었다고 생각했습니다.

그러나 그는 곧 그의 딸이 실제로 임신했다는 사실을 알게 되었다.123

Target의 알고리즘은 특정 구매 패턴을 인식하여 임신을 식별했습니다. 무향 제품, 비타민, 면봉 구매는 임신한 고객에게 흔히 발생했습니다.124 알고리즘에 대해 상당히 우려되는 점은 상대적으로 무해한 데이터에서 민감한 건강 데이터를 추론할 수 있다는 것입니다.

게다가 알고리즘이 추론을 위해 사용한 데이터는 예측하기 어려웠습니다.

따라서 추론은 사람들이 자신의 삶을 관리하는 방법에 대한 전통적인 그림을 뒤집습니다.

---

120 Alicia Solow-Niederman, 정보 프라이버시 및 추론 경제, 117 Nw. L. 개정 357(2022).

121 Solove, 데이터는 데이터가 하는 일입니다. 각주 X, at X.

122 Solow-Niederman, 추론 경제, 위 참고 X, at X.

123 Charles Duhigg, 기업이 귀하의 비밀을 배우는 방법, NY Times Magazine(2012년 2월 16일); CHARLES DUHIGG, 습관 의 힘: 삶 과 사업 에서 우리가 하는 일 을 하는 이유 182-97 , 209-10 (2012).

124 찰스 두히그, 습관 의 힘: 삶 과 사업 에서 우리 가 하는 일을 하는 이유 194 (2012).

은둔. 기계 학습 알고리즘은 데이터 조직이 알고 있는 내용을 사람들이 통제할 수 없을 만큼 놀라운 추론을 너무 많이 할 수 있습니다.125

추론은 정확할 때뿐만 아니라, 틀렸을 때도 해를 끼칠 수 있습니다. AI는 개인의 프로필을 다른 사람의 방대한 데이터 세트와 일치시키고 프로필의 유사성을 식별하여 추론합니다. 따라서 추론은 그것이 옳든 그르든 해를 끼칠 수 있습니다. 정확한 추론은 사람들의 사생활에 대해 너무 많은 것을 노출시킬 수 있으며, 부정확한 추론은 사람들에 대한 잘못된 판단이나 결정을 초래할 수 있습니다.

개인정보 보호법은 추론 과정을 통한 데이터 생성보다는 실제 데이터 수집에 중점을 두는 경향이 있습니다. 대부분의 개인정보 보호법은 개인에게 자신의 데이터를 수정하거나 데이터 수집에 동의할 권리를 부여하지만 일반적으로 개인이 자신의 데이터에서 파생된 추론에 이의를 제기하거나 수정할 수 있도록 허용하는 데는 부족합니다.126

앞에서 설명한 것처럼 추론을 통해 데이터를 생성하는 프로세스는 기본적으로 데이터 수집 작업을 반영합니다. 많은 개인 정보 보호 규정의 핵심 원칙은 조직이 정의된 목적에 필요한 개인 데이터만 수집하도록 제한하는 것입니다. 그러나 조직이 추론을 통해 새로운 데이터를 생성할 수 있다면 데이터 수집에 대한 제한은 다소 환상적이 됩니다.

추론을 통해 생성된 데이터는 대중의 기대를 뒤집고 데이터 수집 제한에 대한 주장을 오해하게 만듭니다. 따라서 법은 추론을 통해 도출된 데이터를 수집된 데이터와 동등하게 취급해야 합니다.

불행하게도 개인 정보 보호법은 데이터 생성을 데이터 수집과 동일하게 취급하지 않습니다. 많은 미국 개인 정보 보호법은 개인으로부터 또는 개인에 관해 수집된 데이터에 중점을 둡니다.127 GDPR 하에서도 Sandra Wachter와 Brent Mittelstadt가 언급한 것처럼 "추론은 데이터 주체가 제공하는 다른 유형의 개인 데이터보다 데이터 보호법에 따라 덜 보호됩니다."128As Mireille Hildebrandt는 EU 법률은 “데이터 처리를 통해 생성되는 새로운 유형의 지식을 파악하지 못한 채 데이터, 개인 데이터 및 그 남용 가능성에 대해 생각하는 전통적인 방식을 기반으로 합니다 . 결론은 개인 데이터에 관한 데이터 보호법이 효과적이라고 하더라도 상관 관계가 있는 데이터의 패턴을 처리하는 방법을 모른다는 것입니다 .” 129

---

125 Solove, 데이터는 데이터가 하는 일이다, 각주 X, at X.

126 마쓰미, 정정의 실패, 각주 X, at X.

127 예를 들어, CCPA는 데이터 수집을 “어떤 수단으로든 소비자와 관련된 개인 정보를 구매, 임대, 수집, 획득, 수신 또는 액세스하는 것”으로 정의합니다. 여기에는 적극적으로든 수동적으로든 소비자로부터 정보를 받거나 소비자의 행동을 관찰하는 것이 포함됩니다.” CCPA 1798.140(f).

128 Sandra Wachter & Brent Mittelstadt, 합리적인 추론에 대한 권리: 빅 데이터 및 AI 시대의 데이터 보호법 재고, 2019 컬럼. 버스. L. Rev. 494, 572 (2019).

129 Mireille Hildebrandt, 유럽 시민 프로파일링 및 정체성, 유럽 시민 프로파일링 : 학제간 관점 303, 321(Mirielle Hildebrandt & Seth Gutwirth eds. 2008).

많은 개인정보 보호법은 개인에게 자신의 데이터를 수정하거나 수집에 동의할 수 있는 권리를 부여하지만, 데이터에서 도출된 추론에 이의를 제기하거나 수정할 수 있는 수단을 거의 제공하지 않습니다. Sandra Wachter와 Brent Mittelstadt는 개인정보 보호법이 개인에게 "합리적인 추론에 대한 권리"를 제공해야 한다고 제안합니다.130
그들은 다음과 같이 주장합니다. "알고리즘이 개인에 대해 '고위험 추론'을 이끌어내는 경우, 이 권리는 데이터 관리자가 추론이 합리적이라는 것을 입증하기 위한 사전 정당성을 제공해야 합니다."131

합리적인 추론을 할 권리가 개인정보 보호법에 긍정적인 발전이 되겠지만 그것만으로는 충분하지 않습니다. 추론하는 AI의 힘은 현재 개인 정보 보호법의 많은 조항과 목표를 논쟁의 여지가 있게 만듭니다. 사람들이 기대하지 않거나 동의하지 않은 새로운 데이터가 추론될 수 있다면 사람들이 자신에 대해 수집된 데이터에 대해 알 수 있고 자신에 대해 알려진 내용과 데이터 사용 방법을 결정할 수 있다는 생각은 더 이상 쓸모가 없습니다. 추론을 할 수 있는 AI의 엄청난 능력은 개별 제어 모델의 작동 불가능성을 극명하게 보여줍니다.

(b) 개인정보 보호에 대한 최종 실행

AI 데이터 생성은 개인정보 보호에 대한 최종 실행으로 이어질 수 있습니다. 개인 정보 보호법은 특정 결정을 위해 수집되는 것을 제외하고 오랫동안 기밀 데이터를 보호해 왔습니다. 예를 들어 의사, 변호사 등 전문적 관계에서 생성된 기밀 데이터는 이러한 관계의 기밀성을 보호하기 위해 판결 결정에서 제외됩니다. 데이터가 더 정확한 결정을 내릴 수 있다고 하더라도 – 재판에서 진실을 확립하는 것이 중요하더라도 – 여전히 특권에 의해 제외됩니다.132 또 다른 예를 들면, 연방 유전 정보 차별금지법(GINA)은 고용주가 다음과 같은 행위를 할 수 없다고 규정합니다. 특정 예외를 제외하고 직원 또는 직원의 가족에 관한 유전 정보를 요청, 요구 또는 구매합니다.133

그러나 AI 기술은 엄청난 추론 능력을 통해 기밀 보호에 따라 제외될 개인 데이터를 생성할 수 있습니다. 기밀 데이터를 탐색하기 위해 추론을 생성할 수 있는 경우 AI는 기밀 데이터 보호를 의미 없게 만들 수 있습니다. 따라서 개인정보 보호법은 기밀 데이터 사용에 대한 제한을 회피하기 위해 추론된 데이터를 사용하는 것을 제한해야 합니다.

또한 AI는 개인 데이터를 비식별화하는 기능을 방해할 수 있습니다. 법학 교수인 Charlotte Tschider가 지적했듯이 AI는 HIPAA, CCPA 등 식별되지 않은 개인 데이터의 사용을 허용하는 다양한 개인 정보 보호법을 다음과 같이 방해할 수 있습니다.

---

130 Wachter & Mittelstadt, 합리적인 추론, 각주 X, at 500.

131 ID. 500-01에서.

132 DANIEL J. SOLOVE 및 PAUL M. SCHWARTZ, 정보 개인 정보 보호법 419-20(8판 2024).

133 42 USC § 2000ff.

데이터의 재식별이 가능하다.134

추론의 문제는 개인 정보 보호법의 완전한 점검을 필요로 합니다. 쉽게 패치할 수 있는 문제는 아닙니다. AI 추론은 데이터 수집을 규제하여 개인 정보를 보호하려는 시도가 충분하지 않음을 보여줍니다. 법은 데이터 생성도 다루어야 합니다.

2. 악의적인 물질

AI는 추론을 넘어 다양한 콘텐츠를 생성할 수 있습니다. 이 콘텐츠 중 일부는 매우 해로울 수 있습니다. AI 챗봇은 사람에 대한 잘못된 사실, 즉 '환각' 현상을 만들어낼 수 있습니다. 일례로, ChatGPT는 교수가 성희롱자라고 허위로 진술했습니다.135 AI는 "딥 페이크"(사람에 대한 현실적인 가짜 사진 및 비디오)를 촉진하는 데 사용될 수 있습니다.136 수많은 경우에 사람에 대한 딥 페이크 포르노 비디오가 제작되고 있습니다. , 대부분 여성으로 인해 엄청난 피해를 입었습니다.137 최근의 예로는 음악 스타 Taylor Swift의 성적으로 노골적인 딥페이크 이미지와 비디오가 바이러스로 유포되는 경우가 있었습니다.138

문제를 더욱 복잡하게 만드는 것은 많은 AI 도구가 대중에게 공개되어 있고 누구나 이를 사악한 목적으로 사용할 수 있다는 것입니다. 악의적인 AI 사용자를 잡아 처벌하기가 어렵고, 수정헌법 제1조에 따른 장애가 있을 수 있을 뿐만 아니라 피해자가 법적 구제를 받기까지 상당한 시간과 비용이 소요될 수 있습니다. 개인 정보 보호법은 유해한 사용을 제한하기 위해 AI 도구 제작자에게 책임을 부여해야 합니다. 그러나 많은 기술 제품이나 서비스와 마찬가지로 사람들이 이를 유해한 방식으로 사용할 경우 법률은 일반적으로 제작자에게 책임을 약하게 부과했습니다. AI도 비슷한 이야기일 것이다.

예를 들어 온라인 플랫폼의 경우 미국 법률에 따라 사용자 콘텐츠에 대한 책임을 지지 않습니다. 통신 품위법(CDA) 제 230조는 사용자의 콘텐츠에 대해 플랫폼을 면제합니다. "대화형 컴퓨터 서비스의 제공자 또는 사용자는 다른 정보 콘텐츠 제공자가 제공한 정보의 게시자 또는 발표자로 취급되어서는 안 됩니다."139

230조의 본문은 좁지만, 법원은 이를 거대한 조항으로 해석합니다.

---

134 Charlotte A. Tschider, AI의 정당한 이익: 공익 개인 정보 보호 모델을 향하여, 21 Hous. J. Health L. & Pol'y 125, 176(2021).

135 Pranshu Verma 및 Will Oremus, "ChatGPT가 성희롱 스캔들을 고안하고 실제 법률 교수를 피고인으로 지명했습니다", Wash. Post(2023년 4월 5일).

136 Robert Chesney 및 Danielle Keats Citron, 딥 페이크: 개인 정보 보호, 민주주의 및 국가 안보를 위한 다가오는 도전, 107 Cal. L. 개정 1753(2019); Mary Anne Franks 및 Ari Ezra Waldman, 섹스, 거짓말 및 비디오테이프: 딥 페이크 및 자유 발언 망상, 78 Md. L. Rev. 892(2019).

137 Jennifer Kite-Powell, “딥페이크가 등장했습니다. 이를 막을 수 있을까요?” 포브스(2023년 9월 20일); CITRON, 개인 정보 보호를 위한 싸움 , 각주 X, 38-39; 메리 앤 프랭크스와 다니엘 키츠 시트론,
음성 기계로서의 인터넷 및 기타 혼란스러운 신화 섹션 230 개혁, 2020 U.
치. 법률 F. 45 (2020).

138 Blake Montgomery, “Taylor Swift AI 이미지로 인해 미국 법안이 합의되지 않은 성적인 딥페이크에 대처하도록 촉구”, The Guardian(2024년 1월 30일).

139 47 USC § 230(c)(1).

플랫폼 사용자의 발언에 대한 면책 부여.140 230항의 원래 목적은 플랫폼이 다른 사람이 제공한 정보에 대해 게시자 또는 발표자로서 책임을 지지 않도록 보장하는 것이었습니다. 이는 타인의 콘텐츠 배포자가 해당 콘텐츠가 명예훼손적이거나 개인 정보 보호를 침해한다는 것을 알고 있거나 알아야 하는 경우 책임을 져야 하는 배포자 책임을 제거하는 것을 목표로 하지 않았습니다.141

그러나 법원은 표현의 자유라는 이름으로 배포자의 책임을 없애기 위해 230조의 범위를 크게 확대했습니다.142 법학 교수 Danielle Citron이 주장한 것처럼, 이 법은 유해한 콘텐츠를 중단하기 위해 어떠한 조치도 취하지 않은 사이트를 보호할 뿐만 아니라 그러한 콘텐츠를 조장하고 조장하는 사이트를 보호합니다.143 법의 보호로 인해 이러한 사이트가 급증했습니다. Citron은 다음과 같이 말합니다. "9,500개가 넘는 사이트에서 치마속 치마, 아래 블라우스, 딥페이크 섹스 비디오와 실제 친밀한 이미지를 포함하여 사용자가 제공한 합의되지 않은 친밀한 이미지를 호스팅합니다." 144

AI는 사기, 사기, 사기를 확대하여 이러한 악성 활동을 증폭시킬 수 있는 능력을 갖추고 있습니다. 예를 들어, 한 여성은 딸로부터 다음과 같은 전화를 받았습니다. “엄마, 저 나쁜 남자들이 저를 갖고 있어요. 도와주세요! 도와주세요!"
납치범들은 처음에 그녀에게 100만 달러를 송금하지 않으면 딸을 해칠 것이라고 요구했습니다. 하지만 그 전화는 가짜였다. 딸의 목소리를 AI 로 흉내내고 있었습니다.145

AI 도구는 가드레일, 보호 장치 또는 사용 규칙이 거의 없는 상태로 대중에게 출시되고 있습니다. 대중은 쉽게 무기화되어 개인에게 광범위한 해를 끼치거나 사회에 치명적인 해를 끼칠 수 있는 강력한 도구로 무장하고 있습니다.146 AI 도구를 대중과 공유하는 것은 민주적일 수 있지만 필연적으로 많은 사람들이 오용할 것이기 때문에 위험할 수도 있습니다. 이 도구들.

AI는 새로운 데이터 보안 취약점을 만들 수 있습니다. AI는 해커와 악의적인 행위자가 공격을 더 잘 수행하고 더욱 악의적인 사기를 저지르는 데 도움이 될 수 있습니다. AI는 취약성을 식별하거나 악성 프로그램을 작성하는 데 도움을 줄 수 있습니다.147 생성적 AI를 통해 해커는 "즉각적 주입"에 참여할 수 있습니다.

---

140 Zeran v. AOL, 129 F. 3d 327(4th Cir. 1997) 참조 ; 또한 DANIEL J.SOLOVE 및 PAUL M. SCHWARTZ를 참조하세요. 정보 개인정보 보호법 167-76 (2024년 8판).

141 다니엘 J. 솔러브(DANIEL J. SOLOVE), 평판 의 미래 : 인터넷 상의 가십 , 소문, 개인 정보 보호 149-160(2007).

142 SOLOVE, FUTURE OF REPUTATION, 위 의 X 참고. DANIELLE KEATS CITRON, HATE CRIMES IN CYBERSPACE (2014) 도 참조하세요 . 섹션 230에 대한 자세한 내용은 JEFF KOSSEFF, 인터넷을 만든 26가지 단어 (2019) 를 참조하세요 .

143 CITRON, 개인 정보 보호를 위한 싸움 , 각주 X, 104.

144 Danielle Keats Citron, 사이버 성 학대의 지속적인 (비)가시성, 133 Yale LJ 포럼 333, 347(2023).

145 Erum Salam, "미국 어머니가 '납치된 딸'로부터 전화를 받았습니다. 하지만 실제로는 AI 사기입니다." 가디언(2023년 6월 14일).

146 Philipp Hacker, Andreas Engel 및 Marco Mauer, ChatGPT 및 기타 대규모 생성 AI 모델 규제 (2023년 5월 12일), https://doi.org/10.48550/arXiv.2302.02337을 참조하십시오 .

147 Chuck Brooks, "인공 지능 및 사이버 보안 입문서", Forbes(2023년 9월 26일).

비공개로 유지되어야 하는 데이터를 노출시킵니다."148 또한 해커는 훈련 데이터를 오염시켜 생성 AI 결과에 영향을 미칠 수 있습니다.

법률은 오랫동안 사기를 범죄로 규정해 왔지만 디지털 범죄는 막기가 상당히 어려울 수 있습니다. 범죄자는 현지 법 집행 기관의 실질적인 손이 닿지 않는 곳이라면 어디든 있을 수 있습니다. AI 도구가 부도덕한 손에 들어가면서 더 큰 규모로 더 많은 사람들을 희생시키는 데 사용될 것입니다. 지금까지 법은 디지털 환경에서 신원 도용 및 사기 피해자를 보호하는 데 매우 부적절했습니다.

나이. [149]

데이터 보안 문제의 경우 법률 개정이 절실히 필요합니다. 많은 개인 정보 보호법에서는 데이터 침해 알림을 통해 데이터 보안을 중점적으로 다룹니다. 여기에는 데이터 침해가 발생한 조직이 규제 기관과 영향을 받은 개인에게 알리도록 하는 요구 사항이 포함됩니다.150 불행하게도 침해 알림은 백신이나 치료법이 아닙니다. 그것은 단지 질병에 대한 알림일 뿐입니다. 기껏해야 침해 알림은 데이터 침해에 대해 더 큰 투명성을 제공하는데, 이는 좋은 일이지만 데이터 보안을 강화하는 것은 아닙니다.

제한된 예외를 제외하고 데이터 보안법은 일반적으로 위반된 조직에만 초점을 맞추고 모든 조직에 책임을 부여하지 않습니다.
책임 당사자. 법률은 위반의 여파에 사로잡혀 필요한 예방 조치를 무시하고 데이터 위반의 영향을 예방하고 완화할 수 있는 위치에 있는 사람에게 책임을 할당하지 않습니다.151

법은 데이터 침해에 기여한 모든 행위자에게 책임을 물을 수 없습니다.152 AI 도구 제작자는 판도라의 위험 상자를 풀어도 그에 따른 이러한 피해에 대한 책임을 회피할 수 있습니다. AI는 법에서 새로운 접근 방식의 필요성을 강조합니다.

3. 시뮬레이션

AI는 AI인 것처럼 위장하여 기만적일 수 있습니다. 사람들은 자신이 인간과 상호 작용하고 있다고 생각하지만 실제로는 기계와 소통하고 있습니다. 인간을 시뮬레이션하는 것은 속임수의 한 형태일 수 있습니다. 인간을 시뮬레이션하면 기계와 상호작용할 때와 인간과 상호작용할 때 도덕적 고려 사항이 다르기 때문에 인간이 다르게 반응하게 됩니다. 법학 교수인 Frank Pasquale는 다음과 같이 주장합니다. "챗봇이 부주의한 사람들을 속여 인간과 상호 작용하고 있다고 생각하게 하면, 프로그래머는 위조자 역할을 하여 기계의 상태를 높이기 위해 실제 인간 존재의 특징을 위조합니다."153

---

148 Trend Micro, "OWASP에 따른 상위 10가지 AI 보안 위험"(2023년 8월 15일), https://www.trendmicro.com/en_vn/ciso/23/h/top-ai-risks.html.
149 Daniel J. Solove, 신원 도용, 개인 정보 보호 및 취약성 아키텍처, 54 Hastings LJ 1227(2003).

150 다니엘 J. SOLOVE & WOODROW HARTZOG, 침해! 데이터 보안법 이 실패하는 이유 와 이를 개선하는 방법 (2022).

151 ID.
152 ID 참조. 81-110에서.

153 프랭크 파스퀄, 로봇공학의 새로운 법칙 : AI 시대 의 인간 전문성 보호 8

최신 AI 도구는 점점 더 Turing 테스트를 통과할 수 있게 되었습니다. 1950년 앨런 튜링(Alan Turing)이 고안한 이 테스트는 인간이 다른 인간이나 기계와 상호 작용하고 있는지 여부를 해독할 수 있는지 조사합니다.154 튜링에게 기계가 지능을 가질 수 있는지에 대한 질문은 "의미가 없습니다". 중요한 것은 기계가 인간을 얼마나 잘 모방할 수 있는가 하는 점이었고, 그는 질문자가 숨어 있는 인간과 기계에게 질문을 하고,

어느 것이 어느 것인지 결정하세요.155

그러나 Turing 테스트에서는 기계가 실제로 지능적인지 여부가 중요하지 않다고 가정합니다. 기계가 사람들을 속여 자신이 인간이라고 믿게 만드는 한 이것으로 충분합니다. 본질적으로 Turing 테스트는 시뮬레이션이 실제처럼 보이는 한 현실은 중요하지 않다고 가정합니다.

하지만 시뮬레이션과 현실에는 큰 차이가 있습니다. 시뮬레이션은 허구입니다. 그것은 특정한 목적과 가정을 가지고 특정한 목적을 위해 인간에 의해 의도적으로 구성되었습니다. 기계가 진정한 지능을 가지고 있는지 여부는 기계의 출력, 결정 및 행동에 대한 책임을 윤리적, 법적으로 할당하는 방법에 영향을 미치기 때문에 중요합니다.

또한 AI가 정말로 지능적이라면 이는 우리가 AI에게 주체성을 인정해야 하는지 여부에 영향을 미칩니다. 아이작 아시모프(Isaac Asimov)의 중편 바이센테니얼 맨 (Bicentennial Man) 에서 로봇은 자신의 자유를 추구하고 획득한 후 인간으로 변할 수 있는 권리를 소송에 참여시킵니다.156 진정한 지능은 최소한 인격에 대한 도덕적, 법적 인정뿐만 아니라 도덕적, 법적 인정도 고려하도록 요구합니다. 자신의 행동에 대한 책임. 그러나 오늘날의 AI는 단지 도구일 뿐이며 전적으로 제작자와 사용자의 책임입니다.

AI는 시뮬레이션이라는 것을 알면서도 조작할 수도 있습니다. 시뮬레이션은 너무나 설득력이 있어서 우리는 그것의 진실성에 너무 매료되어 그것이 실제인 것처럼 행동하는 것을 거부하기가 어렵습니다. 우리는 그것이 현실이 아니라는 것을 알 수도 있지만 여전히 우리의 감정을 촉발하고 다른 방식으로 행동하도록 유도할 수 있습니다. 예를 들어, 우리는 덜 의인화된 기계를 사용하는 것보다 시뮬레이션된 지능을 사용하여 더 큰 신뢰 유대를 형성할 수 있습니다. 예를 들어 영화 그녀 (2013) 에서는 남자가 AI 페르소나와 사랑에 빠진다. 그는 그녀가 진짜가 아니라는 것을 알고 있지만 그럼에도 불구하고 시뮬레이션에 매료되었습니다. 영화는 과연 이 관계가 좋았던 것인지 의문을 제기한다. 주인공은 AI 페르소나가 다른 많은 사람들과 동시에 이야기하고 있으며 수백 명과 사랑에 빠졌다는 사실을 알고 현실로 돌아옵니다. 우리가 AI에 참여하고 있다는 사실을 완전히 투명하게 공개하더라도 이 문제를 완전히 해결할 수는 없습니다.

(2020).

154 앨런 튜링, 컴퓨팅 기계와 지능, 59 Mind 433(1950).

155 ID.

156 ISAAC ASIMOV, 200년의 남자 와 다른 이야기들 (1976).

개인 정보 보호법은 인간과 AI의 상호 작용을 규제해야 합니다. 사람들은 자신이 AI와 상호작용하고 있는지 실제 인간과 상호작용하고 있는지 알아야 합니다. AI의 개입에 대한 투명성을 요구하는 것 외에도 법은 특정 상황에서 AI가 단순한 컴퓨터 코드가 아니라는 점을 인식해야 합니다. 인간 시뮬레이션은 다른 기계 상호 작용과는 달리 매우 강력할 수 있습니다.

D. 의사결정

AI는 종종 개인 데이터를 기반으로 사람에 대한 결정을 내리거나 개인의 개인 생활에 영향을 미치는 데 사용됩니다. 예를 들어, AI 도구는 이력서 평가부터 비디오 인터뷰 분석 수행에 이르기까지 직장 채용 결정에 점점 더 많이 사용되고 있습니다.157 AI는 형사 구금 및 선고 결정에 널리 사용됩니다.158 AI 의사 결정은 인간의 의사 결정과 다르며 임금 인상도 다릅니다. 규제적 관심이 필요한 많은 우려 사항.

1. 예측

AI 도구는 미래에 대한 예측을 위해 자주 사용됩니다. 법학자 마츠미 히데유키와 내가 지적했듯이, 알고리즘 예측은 점점 더 많이 이루어지고 있으며 그 결과와 해악은 충분히 평가되지 않습니다.159

알고리즘 예측은 과거 데이터의 패턴을 기반으로 이루어집니다. 알고리즘 예측에는 두 가지 가정이 있습니다. (1) 역사가 반복되고 과거에 일어난 일은 미래에도 다시 일어날 것입니다. (2) 유사한 특성이나 행동 패턴을 가진 사람들은 다른 면에서도 유사할 가능성이 높습니다.

기계학습 알고리즘과 AI 기술은 과거와 현재에 대한 추론뿐만 아니라 미래 사건을 예측하는 데에도 사용됩니다.160
예측은 추론의 하위 집합이지만 과거 및 현재에 대한 추론과 충분히 구별되므로 특별한 초점과 예측이 필요합니다.
치료.

알고리즘 예측은 단순히 미래를 예측하는 것 이상의 역할을 합니다. 그들은 또한 모양을 만든다

---

157 AJUNWA, THE QUANTIFIED WORKER, 각주 X, 138-70. HILKE SCHELLMANN, 알고리즘 : AI 가 누가 채용되고 , 모니터링되고, 승진되고 , 해고 되는지 결정하는 방법 과 우리가 지금 반격 해야 하는 이유 83-128(2024).

158 BERNARD E. HARCOURT, 예측 반대 : 실제 41-45 세 의 프로파일링, 정책 및 처벌 (2007); Jessica M. Eaglin, 예측 분석의 처벌 불일치, 14 I/S: A J. of L. & Pol'y, 87, 100-01(2017).

159 마츠미 히데유키 & 다니엘 J. 솔로베, 예측 사회: AI와 미래 예측의 문제, 진행 중인 작업.

160 마쓰미 히데유키, 예측과 개인 정보 보호: 개인 정보 사용에 대한 규칙이 있어야 할까요? 미래를 예측하기 위한 데이터?, 48 Cumb. L. 개정 149(2018);

it.161 이러한 알고리즘은 광범위한 데이터 세트를 분석하고 통계적 방법을 사용하여 향후 결과를 예측하는 방식으로 작동합니다. 도주 위험으로 인해 형사 피고인을 재판 전에 구금해야 하는지 여부를 평가하고, 재범 여부를 기준으로 형량을 결정하고, 대출 상환 이력을 기준으로 신용도를 평가하는 등 인간 행동과 관련된 문제에서 알고리즘 예측에 대한 의존도가 증가하고 있습니다. 취업 지원자의 잠재적 성공을 예측합니다.162

이러한 알고리즘 결정은 개인의 기회와 자유에 중대한 영향을 미칩니다. 사람들은 건강 예측으로 인해 일자리를 거부당할 수도 있고, 테러 위험 평가에 따라 강화된 공항 보안을 받게 될 수도 있으며, 예측 치안 전술을 통해 법 집행 조치를 받을 수도 있습니다.163

(a) 인간 행위자에 대한 위협

잠재적인 이점에도 불구하고 알고리즘 예측은 개별 기관에 심각한 문제를 제기합니다. 알고리즘 예측은 사람들이 자신의 길을 개척하는 능력을 제한합니다.

예측 모델에서 도출된 결정은 정당한 절차의 원칙에 도전합니다.164 전통적으로 정의는 개인이 자신이 저지르지 않은 행동에 대해 처벌을 받아서는 안 된다고 규정합니다. 그러나 예측 모델을 사용하면 개인이 수행하지 않았거나 수행하지 않을 수도 있는 행동을 기반으로 판단하고 잠재적인 영향을 미칠 수 있습니다. Carissa Véliz 교수는 이렇게 주장합니다. “날씨를 예측하는 것처럼 인간의 행동을 예측함으로써 우리는 사람을 사물처럼 대합니다. 사람을 존중한다는 것은 자신과 상황을 변화시킬 수 있는 선택 의지와 능력을 인정하는 것입니다.”165

이 문제는 Wisconsin v. Loomis 사건에서 명백히 나타났습니다 . 이 사건에서는 COMPAS(대안적 제재를 위한 교정 범죄자 관리 프로파일링)로 알려진 알고리즘 시스템이 피고를 재범 위험이 높은 것으로 평가하여 형량이 더 길어졌습니다.166 피고는 다음과 같이 주장했습니다. 알고리즘의 예측은 다른 사람의 데이터를 기반으로 했기 때문에 그의 적법 절차 권리가 침해되었습니다.

---

161 Matsumi & Solove, The Prediction Society, 각주 X, at X.

162 ID.

163 ANDREW GUNTHRIE FERGUSON, 빅 데이터 정책 의 부상 (2017); Albert Meijer & Martijn Wessels, 예측적 치안 유지: 장점과 단점 검토, 42 Int'l J. Pub. 관리자. 1031, 1031(2019); Elizabeth E. Joh, 새로운 감시 재량: 자동화된 의심, 빅 데이터 및 경찰 활동, 10 Harvard L. & Pol'y Rev. 15, 15-18(2016); Orla Lynskey, 형사 사법 프로파일링 및 EU 데이터 보호법: 예측 치안의 불안정한 보호, 15 Int'l JL in Context 162, 167(2019); Lindsey Barrett, 합리적으로 의심스러운 알고리즘: 미국 국경에서의 예측 치안 유지, 41 NYU Rev. L. & Soc. 변경 132(2017).

164 CATHY O'NEIL, 수학 파괴 의 무기 : 빅 데이터가 불평등을 증가시키고 민주주의를 위협하는 방법 (2016).

165 Carissa Véliz, AI가 당신의 미래를 예측한다면, 당신은 여전히 자유롭습니까? 유선(2021년 12월 27일).

166 위스콘신 대 루미스, 881 NW2d 749(위스콘신 2016).

그의 특별한 행동이 아닙니다. 위스콘신 대법원은 판사가 알고리즘의 권고를 따를 의무가 없다는 점을 지적하면서 이 주장을 기각했지만, 판사는 여전히 이를 신뢰했습니다 .167

연구에 따르면 개인은 알고리즘 결론을 따르는 경향이 있습니다.
Ben Green은 "사람들은 종종 자동화된 조언에 과도하게 의존하고 알고리즘이 강조하는 요소에 더 큰 비중을 두기 때문에 알고리즘의 조언과 다른 요소의 균형을 안정적으로 맞출 수 없습니다"라고 지적합니다.

Loomis 사건 의 우려를 더욱 가중시키는 것은 COMPAS 알고리즘이 어떻게 작동하는지 공개를 거부하고 제작자가 영업 비밀을 인용했다는 것입니다.169
COMPAS에 대한 후속 분석에서는 흑인 피고인에 대한 편견이 드러났습니다.170

2022년 공상과학 영화 마이너리티 리포트(Minority Report)는 경찰이 시스템을 사용하여 범죄를 예측하고 개인이 실제 범죄를 저지르기 전에 체포하는 소름 끼치는 디스토피아 세계를 보여줍니다. 알고리즘 예측도 비슷한 효과를 가집니다.
그들은 사람들이 행동하기 전에 선제적으로 판단하는 데 사용됩니다.
개인이 스스로 선택하고 아직 저지르지 않은 행위에 대해 처벌할 수 있는 권리입니다. Katrina Geddes가 주장한 것처럼, "알고리즘 예측은 통계 그룹의 구성원인 기본 개인을 효과적으로 처벌합니다."171
사람은 다른 사람이 하는 일이 아니라 자신의 행동을 기준으로 평가되어야 합니다.

(b) 과거를 화석화하다

알고리즘 예측은 미래에 대한 명확한 시각을 제공하는 수정구슬의 역할을 하지 않습니다. 실제로 이러한 예측은 내재된 편견, 차별, 불평등 및 특권을 포함하는 역사적 데이터에서 파생된 확률입니다. 이러한 알고리즘 예측을 기반으로 내린 결정은 과거 패턴을 확고히 하는 경향이 있습니다. 예를 들어, 역사적 인종 차별로 인해 흑인의 체포율과 유죄 판결율이 불균형적으로 높아졌습니다.172

이러한 데이터가 알고리즘에 입력되면 해당 집단의 재범률이 높아질 것으로 예측되어 더 가혹한 형을 선고하게 됩니다. 결과적으로, 알고리즘 예측은 기존의 불평등과 편견을 영속화하고 미래에도 투영할 수 있는 잠재력을 가지고 있습니다.173

---

167 Ben Green, 정부 알고리즘에 대한 인간의 감독을 요구하는 정책의 결함, 45 컴퓨터 법률 및 보안 개정판 1, 7(2022).

168 ID. 9시에.

169 이러한 맥락에서 영업비밀 사용에 대한 비판은 Rebecca Wexler, Life, Liberty, and Trade Secrets: Intellectual Property in the Criminal Justice System, 70 Stan을 참조하십시오. L. Rev. 1343 (2017).

170 Jeff Larson 외, COMPAS 재범주의 알고리즘 분석 방법, 1(2017), https://www.propublica.org/article/how-we-analyzed-the-compas-recidivism-algorithm.

171 Geddes, 법적 주제, 각주 X, at 31.

172 Jessica M. Eaglin, 재범 위험 구성, 67 Emory LJ 59, 72(2017).

173 산드라 G. 메이슨, 바이어스 인, 바이어스 아웃, 128 Yale LJ 2218, 2224(2019); Anupam Chander, The Racist Algorithm?, 115 Mich. L. Rev. 1023, 1036(2017); Pauline T. Kim, 기회 조작, 106 Va. L. Rev. 867, 870 (2020) (AI "시스템은 기존 불평등을 반영하고 역사적 불평등을 강화할 수 있는 방식으로 미래 기회에 대한 정보를 배포할 가능성이 높습니다.

알고리즘 예측은 통계적 규범에 초점을 맞추면서 개인의 고유한 자질과 개인적인 내러티브를 간과하는 경우가 많습니다.174 그러나 역사는 예상치 못한 일에 의해 형성되는 경우가 많아 이러한 예측에 의존하기가 어렵습니다. 나심 니콜라스 탈레브(Nassim Nicholas Taleb)는 이러한 예상치 못한 현상을 유럽인들이 호주를 발견한 후 만난 검은 백조의 이름을 따서 '검은 백조'라고 부릅니다. 그 전에 유럽인들은 모든 백조가 흰색이라고 믿었습니다.

Taleb은 예측을 할 때 겸손의 중요성을 강조하기 위해 이 사건을 언급합니다. 그는 우리가 일상적인 사건을 예측하는 데는 능숙할 수 있지만 특별한 사건을 예측하는 능력은 상당히 제한되어 있다고 제안합니다.175

(c) 자기 성취적 예언

예측은 종종 자기 충족적 예언이 되며, 특히 예상된 결과를 강화하는 행동을 촉발할 때 더욱 그렇습니다. 예를 들어, 특정 특성을 가진 개인이 범죄에 더 취약하다는 예측은 그러한 개인에 대한 치안 강화를 초래할 수 있습니다. 이러한 강화된 조사는 더 많은 체포와 유죄 판결로 이어질 수 있습니다. 이는 반드시 예측이 정확하기 때문이 아니라 법 집행 기관이 프로필에 적합한 사람들을 불균형적으로 표적으로 삼고 있기 때문입니다.176

인간 행동에 대한 예측은 단지 이해를 위해서만 이루어지는 것이 아닙니다. 그것은 행동을 위한 도구입니다. AI는 의사결정 과정과 개입에 사용됩니다. 결과적으로 알고리즘 예측을 통해 조직은 인간 행동을 보다 효과적으로 형성, 제어 및 수익화할 수 있습니다.

(d) 정확성을 넘어서

알고리즘 예측은 기존 개인 정보 보호법 프레임워크에 맞추는 데 어려움을 겪습니다. 예측을 해결하기 위해 제공되는 주요 차량 개인 정보 보호법은 개인에게 수정 권리를 제공하는 것입니다. 개인의 통제에 지나치게 의존하는 문제를 넘어, 잘못된 데이터를 수정할 권리가 있지만, 이 권리는 아직 발생하지 않은 사건과 관련되어 정확하거나 부정확하다고 평가하기 어려운 예측에는 효과가 없습니다.177

알고리즘 예측은 참도 거짓도 아닙니다. 왜냐하면 그 진실성은 실제로 나타난 후에만 확립되기 때문입니다. 예를 들어, 개인이 미래에 범죄를 저지를 것이라는 예측을 반박하는 것이 불가능하다고 생각해 보십시오. 이 예측의 진실성은 사후에만 확실하게 평가될 수 있으므로 현재로서는 사실상 논쟁의 여지가 없습니다.

불이익의 패턴.”).
174 Geddes, 법적 주제, 각주 X, at 5.
175 NASSIM NICHOLAS TALEB, 검은 백조: 매우 불가능한 사건 의 영향 xvii , 149 , 138, 149 (2007).

176 GANDY, CHANCE, 위 각주 X, 124-25.
177 마츠미 히데유키, 수정권, 저자와 함께 보관된 초안.

AI 알고리즘으로(또는 이를 통해 강화된) 의사결정을 규제할 때 법은 프로세스에 초점을 맞추는 경우가 많았습니다. 예를 들어 루미스(Loomis) 사건 에서 법원은 주로 알고리즘 예측 사용과 인간 참여 보장에 관한 투명성 제고에 중점을 두고 기본적인 절차적 보호 장치만 명령했습니다. 그러나 Alicia Solow-Niederman이 지적한 것처럼, 그러한 조치는 대체로 피상적이며 "합법성의 외관"을 투영하는 데에만 도움이 됩니다.178 상황을 표면적으로 향상시키는 미용 공정 솔루션에 안주하는 대신 법은 다음과 같은 문제를 강력하게 해결해야 합니다. 알고리즘 예측. 여기에는 이러한 예측이 공정성을 준수하고 사회의 더 넓은 가치와 일치하도록 보장하는 것이 포함됩니다. 대체로 법은 공정한 결정을 보장하는 것을 목표로 해야 합니다. 사람들에 대한 결정은 전체적인 상황과 개인의 행동 및 특성을 고려하고, 그들을 선택의지를 지닌 고유한 개인으로 대우하면서 공정하게 이루어져야 합니다.

2. 결정과 편견

AI의 결정은 종종 인간의 결정보다 우월하다고 선전됩니다. Orly Lobel이 관찰한 것처럼, "AI는 편향성을 제거하는 힘이 될 수 있으며 차별과 학대를 조기에 감지할 수 있습니다."179 Cass Sunstein에 따르면 알고리즘은 "불공평한 대우를 방지하고 오류를 줄일 수 있습니다." 인간과 달리 알고리즘은 “정신적인 지름길을 사용하지 않습니다. 그들은 통계적 예측 변수에 의존하는데, 이는 인지적 편향에 대응하거나 심지어 제거할 수 있음을 의미합니다.”180

인간의 의사결정은 도전으로 가득 차 있습니다. 사람들은 편견을 가지기 쉽고 제한된 범위의 경험에 의존하며 의사결정 과정이 느리고 비효율적인 경향이 있습니다. 감정적인 영향과 비합리적인 요소가 종종 그들의 선택을 좌우합니다. 또한 인간은 충동적으로 행동할 수 있으며 다양한 인지 편향과 경험적 방법의 영향을 받아 잘못된 결정을 내릴 수 있습니다.181

그러나 AI 알고리즘에는 인간의 의사결정보다 나은지 의문을 제기하는 심각한 결함이 있습니다.182 알고리즘은 질적 요인을 희생하면서 정량화 가능한 데이터를 강조하여 의사결정을 변경합니다. 이는 유리할 수 있지만 상당한 비용이 발생하며 종종 간과되기도 합니다.

인간의 생명을 정량화하는 것은 어려운 일입니다.183 현재 AI 결정에는 인간 복지에 영향을 미치는 결정에 중요한 감정, 도덕성 또는 가치 판단이 포함되어 있지 않습니다. 자동화에 지나치게 집중할 위험이 있습니다.

---

178 Alicia G. Solow-Niederman, 알고리즘 그레이 홀, 5 J. Law & Innovation 116, 124(2023).

179 오를리 로벨(ORLY LOBEL) , 평등 기계: 더 밝은 세상을 위한 디지털 기술 활용 더욱 포용적인 미래 (2022년).

180 Cass R. Sunstein, 알고리즘에 의한 통치? 소음이 없고 (잠재적으로) 편견이 적음, 71 Duke LJ 1175, 1177(2022).

181 DANIEL KAHNEMAN, 빠르고 느리게 생각하기 (2011); 솔로러브와 마츠미, 지독한 인간들, 위의 주 X, X에 있습니다.

182 Jenna Burrel 및 Marion Fourcade, The Society of Algorithms, 47 Annual Rev. Sociology 213, 222-23(2021)(AI 알고리즘이 반드시 인간 의사 결정자보다 나은 것은 아니라고 주장함).

183 Solove & Matsumi, Awful Humans, 각주 X, at X.

윤리적 차원을 무시하면서 요소를 무시합니다.184

AI에서 나타나는 편견이 개별 인간의 편견보다 잠재적으로 더 위험하고 해로울 수 있는 이유는 AI 도구를 광범위하게 사용하여 편견을 체계화하고 중립 기술로 위장할 수 있다는 점입니다. 특정 개인, 심지어 많은 개인이 갖고 있는 편견은 일부 개인이 특정 편견 없이 벗어나 결정을 내릴 때 여전히 극복될 수 있습니다. 이것이 사회 변화가 일어나는 방식입니다. 처음에는 소수의 사람들로 시작하여 시간이 지남에 따라 확산됩니다. 그러나 AI는 편견을 신속하게 체계화하여 편견을 더욱 널리 퍼뜨리고 피할 수 없게 만들어 사회 개선의 움직임을 차단할 수 있습니다.

(a) 편향된 훈련 데이터

AI 알고리즘은 편견이 많은 사회의 데이터를 기반으로 하기 때문에 편견과는 거리가 멀습니다. Meredith Broussard는 다음과 같이 썼습니다. “모든 데이터는 더럽습니다.
185 법학 교수 Sandra Mason은 "인종적으로 불평등한 과거는 반드시 인종적으로 불평등한 결과를 낳을 것"이라고 주장합니다. 186 입력 데이터가 편향되면 결과도 편향될 것입니다. 그녀는 과거 데이터를 바탕으로 백인보다 흑인이 더 많이 체포된다면 "예측 분석을 통해 미래에는 백인보다 흑인에게 더 자주 체포될 것으로 예상할 것"이라고 주장합니다.

편향된 데이터의 문제는 Amazon이 기술 역할 채용을 위한 알고리즘을 만들려고 시도했을 때 명백해졌지만 그 결과는 남성 후보자에게 크게 편향되어 있었습니다. 이러한 편견은 알고리즘이 기존 채용 편견으로 인해 남성에게 편향된 10년치 채용 데이터에 대해 훈련되었기 때문에 나타났습니다.188 자동화된 결정의 품질과 공평성은 기반이 되는 데이터에 의해 직접적인 영향을 받습니다. 이 데이터는 편향에서 자유로운 경우가 거의 없습니다.

기술자인 Cathy O'Neil은 알고리즘 모델은 "단지 데이터로부터 구성되는 것이 아니라 어떤 데이터에 주의를 기울일지, 어떤 데이터를 생략할지에 대한 선택을 통해 구성됩니다. 이러한 선택은 단지 물류, 이익, 효율성에 관한 것이 아닙니다. 그것들은 근본적으로 도덕적입니다.”189 법학 교수 Jesscia Eaglin이 주장한 것처럼, 알고리즘에 사용되는 데이터는 단지 발견되는 것이 아니라 특정한 가치 판단을 통해 선택되고 만들어집니다. 예를 들어, Eaglin은 알고리즘 재범 위험 평가 시스템의 입력 데이터가 "정책 질문"에 달려 있다고 지적합니다.

---

184 Solove & Matsumi, Awful Humans, 각주 X, at X.

185 메러디스 브로서드, 인공 비지능: 컴퓨터가 세상을 오해하는 방법 103 (2018).

186 산드라 G. 메이슨, 바이어스 인, 바이어스 아웃, 128 Yale LJ 2218, 2224(2019).

187 ID. 또한 Anupam Chander, The Racist Algorithm?, 115 Mich. L. Rev. 1023, 1036(2017)을 참조하십시오. (“기존 차별을 반드시 반영하는 실제 데이터 세트에서 훈련되거나 운영되는 알고리즘은 해당 차별을 잘 복제할 수 있습니다.”) Solon Barocas 및 Andrew Selbst, 빅 데이터의 서로 다른 영향, 104 Cal. L. Rev. 671, 682 (2016).

188 AJUNWA, 수량화 된 근로자, 각주 X, 83-84.

189 CATHY O'NEIL, 수학 파괴 의 무기 : 빅 데이터가 불평등을 증가시키고 민주주의를 위협하는 방법 (2016).

누가 위험으로 간주되어야 하는지, 사회가 얼마나 위험을 용인하는지에 대해 설명합니다."190 AI 알고리즘에 사용되는 데이터는 중립적으로 인식될 수 있지만 이는 규범적입니다.

법학 교수인 Talia Gillis는 "입력 오류"라고 표현하면서 입력 데이터에서 개인의 인종, 종교 또는 기타 보호되는 특성에 대한 정보를 단순히 제거하려고 시도하는 것만으로는 깨끗한 결과를 얻을 수 없다고 주장합니다. 그녀는 "개인의 보호되는 특성에 대한 정보는 개인에 대한 다른 정보에 포함되어 있으므로 공식적으로 제외된 경우에도 보호되는 특성이 알고리즘에 '알려질' 수 있습니다."라고 관찰합니다.

(b) 새로운 형태의 차별

AI 알고리즘은 중요하다고 간주되는 속성에 초점을 맞춰 새로운 형태의 차별을 도입할 수 있는 잠재력을 가지고 있습니다. 192 이러한 특성은 인종, 성별, 연령과 같이 전통적으로 인식되는 차별의 기반이 아닐 수도 있지만 키가 작거나 과체중이거나 대머리와 같이 종종 불리하게 여겨지는 특성을 포함할 수 있습니다. 알고리즘에서 사용하는 일부 기준은 비정상적인 상관관계에 따라 임의적으로 나타날 수 있습니다. 예를 들어, 알고리즘이 눈 색깔과 낮은 업무 성과 사이의 연관성을 찾는 경우 이 특성을 선호하지 않을 수 있습니다. 이로 인해 새롭고 바람직하지 않은 범주가 생성되어 개인에게 체계적으로 영향을 미칩니다. 우리는 불변의 특성에 근거한 차별에 직면하는 새로운 종류의 불평등이 증가하는 것을 목격할 수 있습니다. 이러한 형태의 불평등은 알고리즘의 복잡성으로 인해 눈에 잘 띄지 않아 감지하고 해결하기가 더 어려울 수 있습니다.

(c) 편견 해소

법은 근절하기 어려운 편향된 결정을 다루어야 합니다. Anupam Chander가 주장한 것처럼 "알고리즘이 훈련되고 작동되는 현실 세계의 사실은 부당한 차별로 가득 차 있기" 때문에 알고리즘이 차별적인 결과를 낳는 것은 놀라운 일이 아닙니다.193 그는 다음과 같이 주장합니다 . 과거 차별의 유산과 현재의 차별 현실이 스며드는 세상을 위한 알고리즘입니다."194

편향된 결정은 불공정한 결정이므로 실질적인 편향 여부를 검토해야 합니다. 프로세스 기반 요구 사항은 도움이 되지만 충분하지는 않습니다.

---

190 Jessica M. Eaglin, 재범 위험 구성, 67 Emory LJ 59(2017).

191 Talia B. Gillis, 입력 오류, 106 Minn. L. Rev. 1175(2022).

192 Tal Zarsky, 양립 불가능: 빅 데이터 시대의 GDPR, 47 Seton Hall L. Rev. 995, 1012(2017).

193 Anupam Chander, The Racist Algorithm?, 115 Mich. L. Rev. 1023(2017); 또한 엘리자베스 E. 참조. Joh, 기계에 먹이주기: 치안, 범죄 데이터 및 알고리즘, 26 Wm. & 메리 빌 Rts. J. 287, 289 (2017) ("경찰관의 모든 행동 또는 행동 거부와 경찰서가 내리는 모든 유사한 결정은 데이터 생성 방법 및 여부에 대한 결정이기도 합니다.") .

194 ID.

문제를 해결하십시오. 법은 이러한 결정의 본질을 고려하지 않고 불공정한 결정을 다룰 수 없습니다.195

3. 자동화

사랑하고, 느끼고, 공감하는 것이
우리를 살아있게 만드는 것입니다. 비록
AI가 현명할지라도 그것은 여전히
인공 벌집일 뿐입니다.

– 채팅GPT

AI에는 자동화된 데이터 처리가 포함됩니다. 이러한 처리의 특성은 자동화가 데이터를 형성하고 왜곡하는 방식과 개인을 대하는 방식으로 인해 개인 정보 보호 문제를 발생시킵니다. 자동화는 사람에 대한 의사결정의 성격과 영향을 변화시킵니다. 때로는 더 나은 변화를 만들어낼 수도 있지만, 그에 따른 상충관계도 있고 사람들의 고유한 개성을 존중하지 못하는 위축된 결정으로 이어질 수도 있습니다.

(a) 정량화 및 이인화

알고리즘을 훈련하기 위해 데이터를 수집할 때는 반드시 수집해야 합니다. 데이터는 표준화되어야 합니다. 특이한 데이터가 정제됩니다. 계량화할 수 없는 데이터는 쉽게 사용할 수 없습니다. Dan Burk가 주장하는 것처럼 정량적 분석 도구를 위해 데이터 요소를 통합하면 “원래 소스의 고유한 형식과 컨텍스트가 상당 부분 제거됩니다. 호환되지 않는 데이터를 재구성하기 위해 분석 처리는 데이터에 근본적인 탈맥락화를 적용하여 관련 없는 정보와 의미를 제거합니다.”196 정성적 데이터가 제거되고 정량화 가능한 데이터만 남으면 개인의 뉘앙스, 질감 및 고유성이 손실됩니다.197 결정 사람들에 대한 왜곡된 그림을 바탕으로 사람들에 대해 만들어지고 있습니다.

자동화는 인간의 의사결정을 복제하려고 하지만 인간의 사고와 행동의 미묘함과 불규칙성을 포착하는 데 종종 어려움을 겪습니다.198
자동화된 의사결정에는 인간 삶의 다양하고 복잡한 시나리오에 필요한 개인화가 부족할 수 있습니다. 대규모 정량 데이터는 폭넓은 추세와 패턴을 드러낼 수 있지만 개인차와 고유한 특성을 간과하는 경우가 많습니다. 통계의 선구자 Lambert Adolphe Jacques Quetelet

---

195 Andrew D. Selbst와 Solon Barocas는 "불공정" 무역 관행에 관한 FTC 법학이 차별을 해결할 수 있다고 주장합니다. 불공정성 조사는 절차뿐만 아니라 결정의 내용에 초점을 맞출 수 있습니다. Andrew D. Selbst 및 Solon Barocas, 불공정한 인공 지능: FTC 개입이 차별법의 한계를 극복할 수 있는 방법, 171 U. _ (2024).

아빠. L. 목사.

196 Dan L. Burk, 알고리즘 법적 측정, 96 Notre Dame L. Rev. 1147(2020).
197 DANIEL J. SOLOVE, THE DIGITAL PERSON, 각주 X, 49쪽.
198 안드레아 로스, 기계에 의한 시험, 104 Geo. LJ 1245(2016)(형사 판결에서 자동화의 병리 논의).

"관찰되는 개인의 수가 많을수록 신체적이든 도덕적이든 개인의 특수성은 더 많이 사라지고 사회가 존재하고 보존되는 일반적인 사실이 두드러진 관점에 남습니다."199

쉽게 정량화할 수 없는 데이터는 자동화 시스템에서 간과되는 경우가 많습니다.
이 프로세스에는 복잡하고 다양한 삶의 경험을 보다 간단한 패턴 기반 형식으로 추출하는 작업이 포함됩니다. 인간의 경험을 통해 얻은 풍부하고 복잡한 정보는 단순화되어야 합니다. 정량화나 표준화를 거부하는 미묘한 차이가 이 과정에서 손실되는 경우가 많습니다. 하지만 인간의 판단은 종종 여기에 의존하기 때문에 이러한 뉘앙스는 매우 중요합니다. 삶의 풍요로움은 종종 그 독특함과 예측 불가능성에 있으며, 인간 경험의 많은 중요한 측면은 쉽게 정량화하기 어렵습니다. 200 Julie Cohen이 선언한 것처럼, 사람은 "거래, 유전자 표지 및 기타 측정 가능한 속성의 총합으로 환원될 수 없습니다."201

AI 의사결정은 대규모로 매우 효율적으로 작동할 수 있기 때문에 그에 따른 이해관계가 엄청납니다. AI 알고리즘은 기존 편견과 편견을 강화하고 체계화할 수 있는 잠재력을 가지고 있습니다.202 Solon Barocas와 Andrew Selbst는 자동화된 의사 결정 영역에서 중요한 문제를 강조했습니다. 즉, 과거 의사 결정의 편견이 공식화된 규칙으로 코드화되어 체계적인 영향을 미칠 수 있다는 것입니다. 203 편견뿐만 아니라 AI 의사결정의 다른 단점도 증폭되고 뿌리내릴 수 있습니다.

(b) 자동화 규제

자동화 문제를 해결하는 것은 법에 있어 중요한 과제입니다. 자동화된 의사결정을 규제하는 가장 강력한 법률은 GDPR입니다.
개인에게 "프로파일링을 포함하여 자동화된 처리에만 기반한 결정을 받지 않을 권리"를 제공합니다. 204 개인은 "적어도 인간의 개입을 받을 권리가 있습니다. . . 자신의 관점을 표현하고 결정에 이의를 제기하는 것 입니다."205 Meg Leta Jones가 지적한 것처럼 GDPR의 이면에 있는 철학은 "완전히 자동화된 방식으로 개인을 대우하거나 자동화된 대우만을 제공하는 것은 개인을 비인간화하는 것입니다. 개인이기 때문에 기계이기 때문에

199 Lambert Adolphe Jacques Quetelet은 CHRIS WIGGINS 및 MATTHEW L. JONES, How Data HAPPENED: A HISTORY FROM THE AGE OF REATHIS 26 TO THE AGE OF ALGORITHMS 26(2023)에서 인용했습니다.

200 DANIEL J. SOLOVE, THE DIGITAL PERSON, 각주 X, 49; Burk, Algorithmic Legal Metrics, 위 참고 X, 1158.

201 Julie E. Cohen, 조사된 삶: 정보 프라이버시와 객체로서의 주체, 52 Stan. 엘. 개정 1373, 1405(2000).

202 Margot E. Kaminski 및 Jennifer R. Urban, AI 콘테스트에 대한 권리, 121 Colum. L. Rev. 1957, 1981 (2021).

203 Solon Barocas 및 Andrew D. Selbst, 빅 데이터의 이질적인 영향, 104 Cal. L. Rev. 671, 682 (2016),

204 GDPR, 각주 X, 예술. 22(1) ("데이터 주체는 프로파일링을 포함하여 자신에게 법적 영향을 미치거나 이와 유사하게 중대한 영향을 미치는 자동화된 처리에만 근거한 결정을 받지 않을 권리가 있습니다.")

205 ID. 예술 22(3)에서.

오직 계산적인 방식으로만 인간을 대할 수 있습니다."206

미국에서 CCPA는 개인에게 자동화된 의사결정에 관한 일부 권리(예: 탈퇴권, 알고리즘 논리에 대해 배우고 예상되는 결과에 대해 알 수 있는 권리)를 제공합니다.207 몇 가지 다른 주 법률에서는 자동화된 의사결정을 다루고 있습니다. 주로 거부권을 제공함으로써 이루어집니다.208

자동화에 대한 GDPR 접근 방식의 주요 제한 사항은 해당 보호가 자동화를 통해 "유일하게" 내려진 결정으로 제한된다는 것입니다. 그러나 많은 자동화된 프로세스에는 어느 정도 사람의 개입이 필요하므로 이러한 특정 보호 기능을 적용할 수 없습니다. 자동화된 의사결정에 관한 GDPR 제 22조는 자동화된 의사결정에만 국한됩니다. 왜냐하면 오늘날 너무나 많은 의사결정이 인간과 기계의 하이브리드이기 때문입니다. 이는 GDPR을 셀 수 없이 많은 의사결정으로 확장할 것입니다. GDPR 제 22조가 관련된 모든 의사결정에 확장될 수 있기 때문에 미끄러운 경사입니다. 데이터나 계산, 심지어 사람이 통계를 잠깐 본 경우에도 마찬가지입니다. 그러나 자동화된 결정 만으로 선을 긋는 것은 너무 제한적입니다. 자동화가 결정에 중요한 역할을 하는 경우에는 보다 그럴듯한 선이 그려질 수 있습니다.

자동화된 프로세스에 대한 GDPR의 보호는 충분하지 않습니다. 자동화된 프로세스에 대한 GDPR 처리의 가장 큰 구성 요소는 사람의 개입을 요구한다는 것입니다. 그러나 인간과 기계의 조합에 의해 내려지는 하이브리드 결정이 점점 늘어나고 있기 때문에 인간은 이미 참여하고 있습니다. 자동화된 의사결정의 품질과 자동화 문제를 해결하기 위한 조치에 대한 보다 실질적인 요구 사항이 필요합니다.

다양한 법률이 투명성 요구 사항을 통해 자동화된 결정을 관리하려고 시도하지만 이러한 투명성은 진정한 통찰력을 제공하지 못하는 경우가 많습니다.
이러한 결정을 내리는 알고리즘의 복잡성은 일반적으로 일반 사람의 이해를 뛰어넘습니다. 이러한 결정은 개인 정보 보호 규범을 위반하지 않고서는 공개할 수 없는 수백만 명의 개인 데이터에 의존하기 때문에 이러한 결정의 이면에 있는 논리를 단순히 이해하는 것만으로는 충분하지 않습니다. 이러한 알고리즘이 훈련된 데이터에 액세스하지 않으면 특정 자동화된 결정을 평가하는 것이 불가능하지는 않더라도 어려운 작업이 됩니다.

(c) 인간과 기계의 의사결정 통합

개인 정보 보호법은 인간과 기계의 의사 결정을 통합하는 방법을 다루어야 합니다. GDPR은 22조에서 자동화된 처리를 규제하지만 제한적입니다.

---

206 멕 레타 존스(Meg Leta Jones), 인간의 순환에 대한 권리: 컴퓨터의 정치적 구성 자동화와 인격, 47 Soc. 마개. 과학. 216(2017).

207 CCPA, 캘리포니아. 문명 법 § 1798.185(a)(16)(법무장관은 기업이 "의사결정 프로세스에 포함된 논리에 대한 의미 있는 정보는 물론 소비자와 관련하여 프로세스의 예상 결과에 대한 설명"을 공개하도록 규정을 발행하도록 요구합니다. ").

208 Thomas, "개인정보 보호법의 대홍수", 각주 X.

자동화된 데이터 처리를 "전적으로" 수행합니다. 209

제22조는 또한 데이터 주체가 자동화된 처리만을 기반으로 한 결정에 이의를 제기하는 경우 데이터 컨트롤러는 개인의 "권리, 자유 및 정당한 이익"을 위한 보호 장치를 구현해야 하며 "개인의 개입을 얻을 수 있는 권리"를 규정해야 한다고 규정합니다. 컨트롤러는 자신의 관점을 표현하고 결정에 이의를 제기합니다." 210

불행하게도 많은 평론가들이 지적했듯이 인간의 개입은 알고리즘 의사 결정 문제에 대한 효과적인 치료법이 아닙니다.211 Rebecca Crootof, Margot Kaminski 및 Nicholson Price가 관찰한 것처럼 인간과 기계로 구성된 "하이브리드 시스템"은 "모든 인간의 느림이 알고리즘 속도를 가로막고, 인간의 편견이 알고리즘의 일관성을 약화시키거나, 알고리즘의 속도와 유연성이 부족하여 정보를 바탕으로 상황에 맞는 결정을 내릴 수 있는 인간의 능력을 손상시키는 최악의 상황을 너무 쉽게 조장합니다." 212 Margot Kaminski와 Jennifer Urban에 따르면, 인간은 종종 "기계 결정에 대한 과신을 야기하는" "자동화 편향"을 품고 있습니다. 213 인간은 종종 자동화된 결정을 효과적으로 평가하는 데 어려움을 겪고 종종 알고리즘을 따르거나 오류를 간과합니다. 불행하게도 GDPR에는 인간이 자동화된 결정을 어떻게 검토해야 하는지에 대한 구체적인 지침이 부족합니다.214

Ben Green이 적절하게 지적했듯이 인간과 기계의 의사 결정 프로세스는 크게 다르기 때문에 통합은 석유와 물을 혼합하는 것과 비슷합니다.
알고리즘 의사결정은 일관성과 엄격한 규칙 준수를 우선시하는 반면 인간의 의사결정은 '유연성과 재량'을 필요로 합니다. 알고리즘에 대한 인간의 감독을 요구하는 것은 이 두 접근 방식 사이의 "내재된 긴장"을 간과하는 것입니다.215

자동화는 의심할 바 없이 효율성을 제공하지만 실제 상황의 복잡성을 포착하지 못하는 지나치게 단순화되고 왜곡된 판단을 생산하는 대가를 치르게 됩니다. 문제는 기술 자체에 있는 것이 아니라 자동화가 인간의 의사결정보다 우월하고 중립적이라는 성급한 가정에 있습니다. 문제는 기술을 어떻게 인식하는가에서 비롯됩니다. 기술을 인간 의사결정의 결함을 해결하는 만병통치약으로 여겨서는 안 됩니다.

---

209 GDPR 조항. 22

210 GDPR 조항. 22

211 예를 들어 Kaminski, Binary Governance, 위 참고 X(루프에 있는 인간은 자동화된 의사 결정을 개선하지 않음)를 참조하십시오. Kiel Brennan-Marquez, Karen Levy 및 Daniel Susser, 이상한 루프: 자동화된 의사결정에 있어서 인간의 겉보기 개입과 실제 인간 개입, 24 Berkeley Tech.
LJ 745(2019)(루프 속 인간은 단지 외모 때문에 거기에 있을 수 있음); Aziz Z. Huq, 기계 학습 상태의 헌법적 권리, 105 Cornell L. Rev. 1875, 1908–10 (2020) (루프에 있는 인간은 종종 결정의 정확성을 향상시키지 않습니다).

212 Rebecca Crootof, Margot E. Kaminski 및 W. Nicholson Price II, Humans in the Loop, 76 Vand.
L. 목사. 429, 468(2023).

213 Kaminski & Urban, AI에 대한 경쟁 권리, 각주 X, 1961.

214 Crootof, Kaminski, & Price, Humans in the Loop, 각주 X, at 437.

215 Ben Green, 정부 알고리즘에 대한 인간의 감독을 요구하는 정책의 결함, 45 컴퓨터 법률 및 보안 개정판 1, 12(2022).

인간을 자동화된 의사결정의 한계에 대한 치료제로 여겨야 할까요? 대신, 법의 주요 목적은 결정이 공정하도록 보장하는 것이어야 합니다.

E. 데이터 분석

AI는 감시와 식별을 통해 사회적 통제를 엄청난 수준으로 촉진할 수 있습니다. Mustafa Suleyman은 다음과 같이 썼습니다. "뛰어난 규모와 정밀도로 데이터를 캡처하고 활용하는 능력; 실시간으로 대응하여 영토에 걸친 감시 및 통제 시스템을 구축합니다. . . 국가 권력의 한계를 매우 포괄적으로 다시 작성하여 완전히 새로운 종류의 실체를 만들어낼 것입니다."216

1. 감시

1791년 철학자 제레미 벤담(Jeremy Bentham)은 중앙 망루 주위에 감방이 배열된 감옥 구조인 "파놉티콘(Panopticon)"을 고안했습니다. 이 설계는 효율성을 극대화하여 수감자를 감독하기 위해 수많은 경비원의 필요성을 줄이는 것을 목표로 했습니다. 판옵티콘에서 수감자들은 감시당할 것이라는 끊임없는 두려움 속에서 살았고, 이는 유순하고 순응적으로 이어졌습니다.

몇 세기 후, 미셸 푸코(Michel Foucault)는 물리적 감옥 구조를 넘어서는 범감옥 권력의 확장을 인식했습니다.217 그는 사회가 감시 기술의 확산을 통해 스스로 감옥을 건설하고 있으며, 숨어 있는 관찰자가 원격 위치에서 개인을 감시할 수 있게 됨을 관찰했습니다.

오늘날 판옵틱 사회를 향한 궤도는 가속화되고 있습니다. 감시 카메라는 보편화되어 빠르게 증가하고 있으며 원격 관료에 의해 모니터링되고 있습니다. 인터넷은 사람들의 행동의 거의 모든 측면을 추적하여 광범위한 디지털 흔적을 기록합니다. Julie Cohen은 감시 사회의 결과가 자유로운 사상과 민주주의를 제약하고 있음을 기민하게 지적했습니다. 그들은 표현과 지적 탐구의 경계를 무너뜨려 개인의 생각과 행동 방식에 영향을 미칩니다.218

또한 감시는 쉽게 남용될 수 있는 광범위한 권한을 정부에 제공합니다. 감시는 개인의 행동, 사회적 상호 작용, 잠재적으로 모든 말과 행동을 포착하므로 단순한 물리적 검색보다 더 확장됩니다. 감시에는 초기 범위를 초과할 수 있는 광범위한 데이터를 수집할 수 있는 기능이 있습니다. 장기간 관찰하면 개인이 불법적이거나 비윤리적인 행동을 하는 것이 잠재적으로 관찰될 수 있습니다.

---

216 무스타파 술레이만 (MUSTAFA SULEYMAN), 다가오는 물결 : 기술, 권력, 그리고 21 세기의 가장 큰 딜레마 192(2023).

217 MICHEL FOUCAULT, 징계 및 처벌 (Alan Sheridan trans., Vintage Books, 2d ed. 1995) (1977); 또한 OSCAR T. GANDY, THE PANOPTIC SORT: A POLITICAL ECONOMY OF 개인 정보 (1993)(새롭게 떠오르는 디지털 경제의 Panoptic 효과 설명)를 참조하세요.

218 Julie E. Cohen, 조사된 삶: 정보 프라이버시와 객체로서의 주체, 52 Stanford Law Review 1373(2000).

그들을 처벌하거나 불신하게 만드는 구실.

AI 기술은 전례 없는 수준의 대규모 감시를 가능하게 합니다. 이미 많은 사회에는 비디오 및 오디오 감시, 위치 추적, 데이터 수집을 위한 광범위한 인프라가 갖춰져 있습니다. 그러나 영상, 오디오 녹음, 피드, 추적 데이터 및 기타 데이터에는 분석이 필요합니다. Bruce Schneier가 기민하게 주장한 것처럼 "AI는 감시 기술로 캡처한 데이터를 쉽게 분석할 수 있기 때문에 야구계를 변화시킵니다."219 Schneier는 감시(데이터 수집)와 스파이(데이터 분석)를 구별합니다. 감시에는 상당한 인력이 필요하며 이로 인해 감시 범위가 제한됩니다. 그러나 Schneier는 AI를 사용하면 데이터가 "대량으로 모두 검색 및 이해할 수 있게 될 것"이라고 지적합니다. 220 수집된 엄청난 양의 데이터를 모두 조사할 수 있는 사람이 충분하지 않으며, 캡처된 모든 오디오를 듣거나 시청할 수 있는 사람도 충분하지 않습니다. 모든 감시 영상. 하지만 AI는 이 모든 것을 할 수 있다. 슈나이어는 다음과 같이 썼습니다.

> 요약은 현대 생성 AI 시스템이 잘하는 일입니다.
> 한 시간 동안 회의를 하면 말한 내용에 대한 한 페이지 요약이 반환됩니다. 수백만 개의 대화를 검색하고 주제별로 정리하도록 요청하면 그렇게 됩니다. 누가 무엇에 대해 이야기하고 있는지 알고 싶으십니까? 그것이 당신에게 말해줄 것이다.221

감시는 AI 이전부터 시작된 문제로, 법은 일반적으로 이를 효과적으로 처리하지 못했습니다. AI는 감시의 피해를 놀라운 수준으로 증폭시킬 것입니다.

2. 신분증

AI는 눈, 얼굴, 걸음걸이, 음성 및 기타 신체적 특성을 기반으로 식별을 용이하게 합니다. AI는 사람들이 하는 행동과 말의 많은 부분에서 독특한 패턴을 감지할 수 있어 수많은 식별 방법을 가능하게 할 수 있습니다.

개인을 쉽게 식별할 수 있으면 정부의 권력이 증폭되어 사회 질서를 향상시킬 수 있지만 억압의 도구로 사용될 가능성도 있습니다. 신원 확인을 통해 정부는 불리하게 여기는 개인을 표적으로 삼고 구금하기가 더 쉬워집니다.

식별이 체계적이고 은밀하게 이루어지면 오용의 위험이 상당히 높아집니다. 정치학자 Richard Sobel이 지적한 것처럼, 식별 시스템은 역사적으로 사회 통제와 차별을 위해 사용되었습니다.222 예를 들어, 노예들은 여행 시 신분증을 휴대하도록 강요받았고, 나치는

219 Bruce Schneier, 인터넷으로 대량 감시가 가능해졌습니다. AI가 대량 감시를 가능하게 합니다, Slate, 2023년 12월 4일.

220 ID.

221 ID.

222 Richard Sobel, 국가 식별 시스템에 따른 정치적 정체성의 저하, 8 BUJ Sci. & 기술. L. 37, 39(2002).

유대인을 찾기 위해 신분증을 사용했고, 르완다의 대량 학살은 식별자 시스템에 의해 촉진되었습니다. 정부 관리들은 부적절한 감시를 위해 이러한 기록을 오용할 수 있습니다. 데이터는 현재의 모든 충동에 적응할 수 있는 권력을 가진 사람들을 위한 다목적 도구가 됩니다. 주목할만한 예는 인구조사국이 제2차 세계 대전 중 일본계 미국인의 억류를 지원하기 위해 1940년 인구 조사 데이터를 사용한 것입니다.223

전 세계적으로 사회는 적절한 예측이나 보호 장치 없이 이러한 현실을 향해 빠르게 움직이고 있습니다. AI는 우리가 이 방향으로 경주할 때 바퀴에 윤활유를 칠할 것입니다. 최근 얼굴 인식의 발전은 이미 우리를 디스토피아적인 미래로 나아가게 만들고 있습니다. 얼굴 인식을 사용하면 감시 영상을 특정 개인과 쉽게 연결할 수 있으므로 감시가 더욱 강력해집니다. 안면 인식 기술을 구현하려는 법 집행 기관과 기업의 노력은 부정확성과 대중의 반발을 포함한 난제에 부딪혔고, 이로 인해 그러한 많은 계획이 포기되었습니다.224

이러한 어려움에도 불구하고 기술은 마치 어둠 속에서 번성하는 곰팡이처럼 지속되고 발전해 왔습니다.

AI 얼굴 인식은 개인의 익명성에 심각한 위협이 됩니다. Woodrow Hartzog와 Evan Selinger는 "얼굴 인식은 억압을 위한 완벽한 도구"라고 썼습니다. 225

AI의 영향을 받는 다른 개인 정보 보호 문제와 마찬가지로 AI의 주요 영향은 증폭입니다. AI는 감시 사회의 완벽함, 즉 광범위한 감시를 총체적인 통제로 전환하겠다고 위협하는 단계를 나타냅니다. 법은 오랫동안 감시 및 식별에 대한 적절한 통제와 감독을 제공하지 못했습니다. AI는 이 실패를 더욱 비극적으로 만들겠다고 위협합니다.

3. 해석과 해독

AI는 정부가 보유하고 있는 데이터의 해석도 용이하게 할 수 있다.
예를 들어, 정부가 암호화된 파일을 찾아 AI 도구로 해독했다고 가정해 보겠습니다. Orin Kerr는 "수정헌법 제4조는 이미 획득한 통신에 대한 인지적 이해 가 아니라 통신에 대한 정부의 접근을 규제 "하기 때문에 암호화가 수정헌법 제4조의 프라이버시에 대한 합리적인 기대를 형성하지 못한다고 주장합니다. 226 이러한 추론에 따라 정부가 개인의 DNA가 있는 항목을 발견하면 , 정부는 수정헌법 제4조의 보호 없이도 DNA를 분석할 수 있습니다. AI가 제공할 것

223 ERIK LARSON, 벌거 벗은 소비자: 어떻게 우리의 개인 생활이 공공 상품이 되는가 53-54(1992)를 참조하십시오 .

224 HILL, YOUR FACE BELONGS, 각주 X 참조.

225 Woodrow Hartzog & Evan Seligner, 얼굴 인식은 억압을 위한 완벽한 도구입니다. Medium(2018년 8월 2일), https://medium.com/@hartzog/facial-recognition-is-the-perfect-tool-for-oppression-bc2a08f0fe66; Lindsey Barrett, 아동 및 기타 모든 사람을 위한 안면 인식 기술 금지, 26 BUJ Sci. & 기술. L. 223(2020).

226 Orin S. Kerr, 사이버 공간의 제4차 수정안: 암호화가 개인 정보 보호에 대한 합리적인 기대를 창출할 수 있습니까?, 33 Conn. L. Rev. 503(2001).

정부는 수정헌법 제4조의 감독 및 제한적 보호를 회피하면서 사람에 대한 데이터를 발견하는 새로운 능력을 갖게 되었습니다.

커(Kerr)는 "헤겔의 지저분한 필체 또는 이해"를 해독하기 위해 법 집행 기관에 영장을 요구하는 불합리한 예를 제공합니다.
분명히 경찰이 어떤 종류의 데이터 분석을 할 때마다 수정헌법 제4조가 발동되어서는 안 됩니다. 왜냐하면 이는 수수께끼를 푸는 것과 유사하게 조사의 거의 모든 측면으로 확장될 수 있기 때문입니다. 정부가 프랑스어로 작성된 메모를 발견하면 이를 영어로 번역하기 위해 수정헌법 제4조 영장을 요구하는 것은 어리석은 일입니다.

그러나 AI는 이러한 사례를 해석하고 해독할 수 있는 믿을 수 없을 정도로 정교한 능력으로 전환합니다. 지저분한 필기와 같은 어처구니없는 상황으로 미끄러질 위험이 있는 것처럼 AI도 반대 방향으로 미끄러운 경사를 만듭니다. 예를 들어, 정부는 인터넷에서 식별되지 않은 데이터를 수집하고 이를 AI로 재식별할 수 있습니다. 정부는 AI 시스템을 사용하여 온라인에서 보유하거나 찾은 데이터로부터 개인에 대한 광범위한 데이터를 추론할 수 있습니다.

이 때문에 법은 커가 지지하는 것과 같은 단순하고 절대적인 규칙을 고수할 수 없습니다. 어디선가 선을 그어야 하는데, 정도나 크기 등의 문제를 다룰 때 선을 그을 정확한 지점이 거의 없기 때문에 어려울 것입니다.

이 토론은 AI가 법에 제기하는 많은 문제의 본질을 포착합니다. AI는 상황을 크게 바꿀 정도로 볼륨을 높입니다. AI는 종종 법칙을 힘의 역설과 혼동합니다. 모래알을 제거한다고 해서 힘이 더 이상 힘이 아니라는 의미는 아닙니다. 알갱이를 하나씩 제거하면 모래가 더미가 아니라고 말할 수 있는 좋은 점이 전혀 없는 것 같습니다.

4. 제한 및 감독

정부 감시 및 데이터 수집과 관련된 AI 사용으로 인해 제기되는 우려는 기존 법률의 심각한 단점을 수정함으로써 가장 잘 해결됩니다. 미국 대법원의 일련의 불행한 결정으로 인해 정부 감시 및 데이터 수집에 대한 수정헌법 제4조의 보호가 사라졌습니다. 현재 정부는 인터넷에서 데이터를 수집하거나 상업 기관으로부터 데이터를 구매하는 데 거의 제한을 두지 않습니다.228

"제3자 원칙"으로 알려진 일련의 사건에서 미국 대법원은 제3자에게 공개된 데이터에 대한 개인 정보 보호에 대한 합리적인 기대가 없다고 판결했습니다. 예를 들어, 연방 대리인이 통지 없이 피고의 은행 기록을 입수한 미국 v. Miller 사건. 법정

227 ID.

228 Matthew J. Tokson, 개인 데이터의 정부 구매, 곧 출간될 Wake Forest L. Rev.(2023), 초안 p. 4, https://ssrn.com/abstract=4574166 (“경찰관은 일반적으로 헌법상의 제한 없이 대중이 이용할 수 있는 물품을 구매할 수 있습니다.”); Orin Kerr, 구매 데이터 및 제4차 수정안, Hoover Inst., (2021년 11월), https://www.hoover.org/sites/default/files/research/docs/kerr_webreadypdf.pdf.

데이터가 "제3자에게 공개"되었기 때문에 은행이 보유한 금융 기록에 대한 개인 정보 보호에 대한 합리적인 기대가 없다고 판결했습니다. 229 Smith v. Maryland 사건 에서 법원은 이후 펜 기록기 사용에 있어 개인 정보 보호에 대한 합리적인 기대가 없다고 판단했습니다. 데이터가 전화 회사에 전달되었기 때문입니다.230 Carpenter가 제3자 원칙의 적용 범위를 어느 정도 축소했지만 법원은 이를 뒤집지 않았습니다.231

궁극적으로 이 법은 정부가 감시에 참여하고 데이터를 수집하고 구매할 수 있도록 허용합니다. 현재 수정헌법 제4조는 정부가 개인 데이터를 저장할 수 있는 기간과 분석 방법에 대해 거의 제한을 두지 않습니다 .232 수정헌법 제4조는 부당한 수색과 압수를 방지하고 정부가 데이터를 획득한 후 데이터에 어떤 일이 발생하는지 에 대해 거의 언급하지 않습니다 .233 즉, 흔히 해석되고 적용되는 방식으로 수정헌법 제4조는 주로 데이터 수집에 초점을 맞추고 데이터 분석을 무시합니다. 234 AI는 정부가 수집한 데이터로 할 수 있는 일의 힘을 높입니다.

수정헌법 제4조나 법적 보호가 정부가 보유하고 있는 데이터에 대한 분석을 제한하려고 한다면, 어디에서 선을 그어야 하는가가 주요 과제가 될 것입니다. 확실히, 법집행관은 범죄를 수사하기 위해 데이터를 분석할 수 있어야 합니다. 하지만 AI는 지금까지 전례 없는 수준으로 데이터 분석을 수행하기 때문에 어딘가에 선을 그어야 합니다.

법은 정부가 과도한 피해나 위험을 초래하는 방식으로 AI 시스템을 사용할 수 없도록 보장해야 합니다. 사용에 대한 일련의 규칙과 오용에 대한 책임뿐만 아니라 지속적으로 독립적인 감독이 있어야 합니다.

그러나 현재 AI 도구를 사용하면 법 집행관은 원하는 것은 무엇이든 사고 원하는 대로 사용할 수 있는 장난감 가게의 어린이와 같으며 감독이나 책임이 거의 없습니다. 정부 감시, 데이터 수집 및 기술 사용을 규제하는 법의 문제로 인해 법은 AI에 대한 준비가 전혀 되어 있지 않습니다. 수정헌법 제4조는 “불합리한 수색 및 압수”를 금지하는 광범위하고 개방적인 방식으로 초안이 작성되었지만, 이를 통해 문제가 되는 엄청난 양의 개인정보 침해 활동에 적용할 수 없게 만드는 협소하고 근시안적인 방식으로 해석되었습니다.

---

229 미국 대 Miller, 425 US 435, 443(1976).

230 Smtih v. Maryland, 442 US 735, 737(1979).

231 United States v. Ellison, 462 F.3d 557 (6th Cir. 2006) (법 집행 데이터베이스를 검색하는 것은 수정헌법 제4조 위반이 아닙니다).

232 United States v. Ellison, 462 F.3d 557 (6th Cir. 2006) (법 집행 데이터베이스를 검색하는 것은 수정헌법 제4조 위반이 아닙니다); Daniel J. Solove, 디지털 서류 및 제4차 수정안 개인 정보 보호의 소멸, 75 S. Cal. L. Rev. 1083, 1166 (2002)(“일단 정보가 수집되면 수정헌법 제4조의 감독 구조는 더 이상 적용되지 않습니다.”).

233 William J. Stuntz, OJ Simpson, Bill Clinton 및 Transsubstantive 제4차 수정안, 114 Harv. L. Rev. 842, 848 (2001) (“수정헌법 제4조는 정보를 밝히려는 정부의 노력을 규제하지만 정부가 밝혀낸 정보로 무엇을 할 수 있는지에 대해서는 언급하지 않습니다.”).

234 Daniel J. Solove, 데이터 마이닝 및 보안 자유 논쟁, 74 U. Chi. L. 개정 343(2008).

기술. 법학 교수인 Fred Cate는 다음과 같이 지적합니다. “정부 데이터 마이닝 프로그램이 확산되고 있음에도 불구하고 의회는 그러한 프로그램을 수행하는 방법에 대한 법적 틀을 제공하거나, 이로 인해 피해를 입은 무고한 사람들에게 보상을 제공하거나, 방법을 명시하는 법안을 제정하지 않았습니다. 그 과정에서 프라이버시가 보호되어야 한다.”235

F. 감독, 참여 및 책임

1. 투명성

개인정보 보호법의 핵심은 투명성입니다. 조직은 수집하는 데이터와 이를 사용하는 방법을 투명하게 공개해야 합니다. 투명성은 AI에 큰 과제를 안겨줍니다. Frank Pasquale이 주장한 것처럼 많은 알고리즘은 "비밀"이며, 이를 사용하면 우리 삶에 대한 중요한 결정이 설명되거나 설명될 수 없는 "블랙박스 사회"에서 우리가 살아가게 됩니다.236 Margot Kaminski는 다음과 같이 말합니다. 알고리즘 책임 거버넌스에서 명확한 위치를 차지합니다.”237 그러나 그녀는 정확히 무엇이 투명해야 하는지에 대해 논쟁이 있다고 지적합니다. 자동화된 프로세스의 존재에 대한 기본적인 알림이 있어야 합니까? 알고리즘 코드, 즉 논리에 대한 투명성이 있어야 합니까? 아니면 알고리즘이 훈련된 데이터를 공개해야 합니까?

일반 데이터 보호 규정(GDPR)은 어느 정도의 알고리즘 투명성을 포함하여 자동화된 처리와 관련된 특정 권리를 도입합니다.238 이러한 조항에 따라 데이터 관리자는 자동화된 의사 결정의 사용에 대해 개인에게 알리고, 데이터에 대한 의미 있는 통찰력을 제공해야 합니다. 이러한 프로세스의 논리를 설명하고 잠재적인 결과를 설명합니다.

투명성이 정말로 의미가 있으려면 자동화된 결정을 이해할 수 있어야 합니다. 기계 학습 알고리즘이 내리는 결정은 복잡할 수 있기 때문에 이것은 기계 학습 알고리즘의 과제입니다.239 Suleyman은 AI 알고리즘이 "설명할 수 없다"고 지적합니다. 알고리즘은

---

235 Fred H. Cate, 정부 데이터 마이닝: 법적 프레임워크의 필요성, 43 Harv. 문명 아르 자형. 문명 LL 개정 435, 461(2008).

236 프랭크 파스퀄, 블랙 박스 사회 : 돈과 정보를 통제하는 숨겨진 알고리즘 218 (2015); Charlotte A. Tschider, "블랙박스 너머", 98 Denv. L. Rev. 683, 699(2021); W. 니콜슨 프라이스, 블랙박스 의학, 28 Harv. 제이엘앤테크. 419, 421(2015).

237 Margot E. Kaminski, 설명할 권리, 설명, 34 Berkeley Tech. 엘제이 199(2019).

238 GDPR 조항. 13, § 2(f), 40-41; ID. 미술. 14, § 2(g), 41-42(정보 주체에게 "22(1)조 및 (4)조에 언급된 프로파일링을 포함한 자동화된 의사 결정의 존재에 대해 알리도록 요구하고, 적어도 해당 조항에서는 사례, 관련된 논리에 대한 의미 있는 정보, 정보 주체에 대한 그러한 처리의 중요성 및 예상되는 결과.”) id도 참조하세요. 미술. 15, § 1(h), 43.

239 캐롤린 켐퍼, 카프카에스크 AI? 머신러닝 시대의 법적 의사결정, 24 Intel. 제안 및 기술 LJ 251, 275 (2020) (“ML 알고리즘의 복잡한 설계, 복잡한 학습 기술, 알고리즘 구조에 영향을 미치는 대량의 데이터로 인해 특정 결과가 얻은 이유를 추적하기가 어렵습니다.”).

구체적인 예측."240 AI 알고리즘은 동적이며 수많은 개인의 집단 데이터에 의존합니다. 개인에 대한 특정 결정을 완전히 이해하려면 개인 데이터와 알고리즘 논리뿐만 아니라 알고리즘이 처리한 다른 사람의 데이터도 알아야 합니다.

그러나 이렇게 광범위한 데이터 세트를 공개하면 다른 개인의 개인정보가 침해될 위험이 있습니다.

이러한 결정이 투명하게 이루어지더라도 여전히 문제가 있을 수 있고 잠재적으로 불공정할 수 있습니다. 따라서 투명성은 데이터 보호의 중요한 측면이지만 알고리즘 의사결정과 관련된 수많은 문제를 해결하기에는 그것만으로는 충분하지 않습니다.241 이러한 시스템이 피해를 입히지 않고 공정하게 작동하도록 보장하려면 추가 조치가 필요합니다.

더욱이, 투명성이 있음에도 불구하고 대부분의 개인은 복잡한 알고리즘을 평가할 준비가 되어 있지 않습니다. 많은 경우, 알고리즘을 이해하려면 알고리즘이 활용하는 훈련 데이터에 접근해야 하는데, 이는 이해하기는커녕 쉽게 이용 가능하거나 생산할 수 없는 경우가 많습니다.242 이 데이터는 사람들의 개인정보를 침해하지 않고는 공개할 수 없는 경우가 많습니다. 이러한 데이터 세트에 포함된 데이터의 양은 개인이 처리하기에는 너무 방대합니다.

또한 많은 알고리즘은 동적이며 새로운 데이터를 기반으로 지속적으로 학습하고 진화하므로 지속적인 평가가 필요하며 이는 대부분의 개인에게 실제로 실행 불가능합니다. 이러한 복잡성은 데이터 사용 및 알고리즘 의사 결정의 광범위한 영향을 다루는 데 있어 현재 개인 정보 보호 권리의 한계를 더욱 강조합니다. 전문가조차도 알고리즘이 특정 결과를 생성하는 이유를 이해하는 데 어려움을 겪습니다. 243 기술자인 Joy Boulamwini는 다음과 같이 말합니다. "신경망의 주요 과제는 훈련 과정에서 컴퓨터 과학자들이 왜 일부 가중치는 강화되고 다른 가중치는 약화되는지 정확히 알지 못한다는 것입니다."244

영업 비밀 보호로 인해 알고리즘 투명성이 방해받을 수 있습니다. 법학 교수인 Charlotte Tschider는 "AI 결정이 어떻게 이루어지는지 설명하는 것은 필요한 공개 정도에 따라 알고리즘의 영업 비밀 상태를 파괴할 가능성이 높습니다."라고 말했습니다. 245 영업 비밀은 알고리즘 작성자가 조사로부터 알고리즘을 보호하기 위해 사용할 수 있습니다. . 루미스 사건 의 경우 재범 위험 분석 도구인 COMPAS를 개발한 회사의 영업비밀

---

240 SULEYMAN, THE COMING WAVE, 각주 X, 143.

241 Devin R. Desai & Joshua A. Kroll, 신뢰하되 검증하세요: 알고리즘 및 법칙 가이드, 31 Harv. 제이엘앤테크. 1, 64 (2017) (투명성만으로는 알고리즘 문제에 대한 충분한 보호가 되지 않음); Andrew D. Selbst & Solon Barocas, The Intuitive Appeal of explainable Machines, 87 Fordham L. Rev. 1085, 1088 (2018) ("기술 시스템에 대한 설명은 필요하지만 법과 정책 목표를 달성하기에는 충분하지 않습니다.")

242 Dennis D. Hirsch, 개인 통제에서 사회 보호까지: 예측 분석 시대의 개인정보 보호법에 대한 새로운 패러다임, 79 Md. L. Rev. 439, 445(2020).

243 Tschider, AI의 정당한 이익, 각주 X, 130.

244 조이 볼람위니 (JOY BOULAMWINI), AI 가면 벗기기 : 기계 의 말 속에서 인간을 보호 하는 나의 임무 53 (2023).

245 Tschider, 블랙 박스, 위 각주 X, 711.

피고인이 도구를 분석하는 것을 방해했습니다.246 법학 교수인 Rebecca Wexler는 형사 사건에서 영업 비밀을 사용하는 것이 "순수한 금전적 이익을 생명과 자유와 동등하게" 두기 때문에 비판했습니다.247

궁극적으로 투명성은 AI의 문제가 될 것이지만 이를 포기해서는 안 됩니다. 개인정보 보호법은 투명성에 지나치게 의존하는 것을 피해야 합니다. 하지만 투명성은 중요하며, 훈련 데이터는 공개할 수 없더라도 그에 대한 세부정보는 공개할 수 있습니다. AI 알고리즘은 연구원과 전문가가 조사할 수 있습니다.

2. 적법절차

앞서 언급했듯이 AI는 개인의 정당한 절차를 위협할 수 있다. Danielle Citron이 주장한 것처럼 "자동화는 의미 있는 통지와 의견을 들을 수 있는 기회에 대한 적법 절차 보장을 위태롭게 합니다."248 Frank Pasquale와 함께 Citron은 신용 평가에 더 큰 적법 절차가 필요하다고 주장합니다. 채점 알고리즘 자체(일종의 기술 기반 규칙 만들기)뿐만 아니라 알고리즘 예측(기술 기반 판결)을 기반으로 한 개별 결정에도 적용됩니다.”249

Margot Kaminski와 Jennifer Urban은 미국에서 "알고리즘 의사결정에 관한 규제 제안은 위험 완화를 목표로 하는 시스템 전반의 규제를 선호하는 개별 정당한 절차에 대한 요구를 크게 무시했습니다"라고 지적했습니다. 250 그들은 EU에서 다음과 같이 주장합니다. GDPR은 개인에게 AI 결정에 이의를 제기할 권리를 제공합니다. “GDPR은 체계적 거버넌스 조치와 데이터 주체에 대한 다양한 개인 권리(투명성, 통지, 액세스, 처리에 반대할 권리, 자동화된 의사 결정 대상에 대한 권리)를 모두 통합합니다. , 특정 결정 에 이의를 제기할 권리 .”251

미국도 비슷한 보호를 받아야 합니다. Kate Crawford와 Jason Schultz에 따르면 중립적인 당사자는 개인의 불만사항을 조사해야 합니다.252

법은 여전히 개인이 발언권을 갖고 불만 사항을 판결할 수 있는 여지를 제공해야 하지만, 법은 보호의 대부분을 개인의 문제에 두는 것을 피해야 합니다. 이는 개인에게 너무 많은 부담을 주고 실행 불가능한 개인 통제 모델을 너무 많이 고수하기 때문입니다.

---

246 위스콘신 대 루미스, 881 NW2d 749(위스콘신 2016).

247 Rebecca Wexler, 생명, 자유, 영업 비밀, 70 Stan. L. Rev. 1343, 1402 (2018).

248 Danielle Keats Citron, 기술 적법 절차, 85 Wash. UL Rev. 1249(2007).

249 Danielle Keats Citron 및 Frank Pasquale, The Scored Society: 자동화된 예측을 위한 적법 절차, 89 Wash. L. Rev. 1 (2014).

250 Kaminski & Urban, AI 콘테스트에 대한 권리, 각주 X, at X.

251 ID. X에서.

252 Kate Crawford 및 Jason Schultz, 빅 데이터 및 적법 절차: 예측적 개인 정보 보호 피해를 시정하기 위한 프레임워크를 향하여, 55 BCL Rev. 93(2014).

3. 이해관계자 참여

학자들은 주요 결정이 모든 관련 이해관계자의 참여가 부족한 경우가 많기 때문에 독점적인 방식으로 AI의 잠재적 개발에 대한 우려를 제기합니다.
AI 시스템은 특히 정부가 사용할 때 소외된 집단에 심각한 영향을 미치는 경우가 너무 많습니다.

예를 들어 미결 구금 알고리즘의 경우 Ngozi Okidegbe 법학 교수는 경제적으로 불리한 배경과 소수 인종 출신의 개인이 이러한 알고리즘의 거버넌스에서 제외될 수 있다고 강조합니다. 그것과 상호작용할 가능성이 높다."253

Alicia Solow-Niederman은 "AI 분야에는 민주적으로 책임 있는 거버넌스 모델에 필요한 적극적인 대중의 목소리가 빠져 있습니다. . . . 모든 협상은 민주적으로 책임 있는 조정이나 상업적 이익 동기에 대한 집행 가능한 점검 없이 규제되지 않은 시장에서 이루어질 것입니다."254

AI는 수많은 이해관계자의 개인 정보 보호에 영향을 미치고 AI 알고리즘은 종종 개인 데이터에 대해 훈련되기 때문에 그러한 알고리즘의 작성자에게 그룹 및 협회로 대표되는 이해관계자의 의견을 고려할 의무를 부과하는 법률에 대한 정당성이 있습니다.

4. 책임

AI를 규제하는 또 다른 접근 방식에는 거버넌스 및 책임 메커니즘의 구현이 포함됩니다. 개인 정보 보호법에는 개인 정보 보호 책임자 임명, 개인 정보 보호 영향 평가 수행, 서면 정책 및 절차 수립, 데이터 관행의 투명성, 문서화 등을 포함하는 이러한 조치가 포함되는 경우가 많습니다. 개인 정보 보호 측면에서 효과적인 것으로 입증된 이러한 메커니즘은 AI를 규제하는 데에도 적용될 수 있습니다.

Pauline Kim은 "편향의 원인은 종종 코드에 있는 것이 아니라 보다 광범위한 사회적 프로세스에 있기 때문에 기술적 도구만으로는 차별적인 알고리즘을 확실하게 방지할 수 없습니다."라고 주장합니다 . 즉, 감사를 통한 자동화된 의사 결정 프로세스입니다."256

Talia Gillis와 Josh Simons에 따르면, 책임은 "중심이 되어야 합니다.

---

253 Ngozi Okidegbe, 알고리즘의 민주화 가능성?, 53 Conn. L. Rev. 739(2022).
254 Alicia Solow-Niederman, 인공 지능 관리, 93 S. Cal. L. 개정 633(2020).
255 Pauline T. Kim, 차별에 대한 감사 알고리즘, 166 U. Pa. L. Rev. Online 189, 202 (2017).

256 ID.

머신러닝을 사용해 의사결정을 관리하는 모든 접근 방식의 목표입니다."
그들은 다음과 같이 자세히 설명합니다. "책임 구조는 기관이 더 주의 깊게 의사결정 절차를 개발하고, 광범위한 이해관계와 관점을 고려하며, 더 많은 종류의 위험과 가능한 피해를 평가하도록 장려할 수 있습니다." 257 Gillis와 Simons는 "책임의 가치 중 일부는 행위가 정당화되어야 한다는 것을 알기 때문에 권력을 가진 사람들의 행위를 변화시킨다는 것"이라고 적절하게 주장합니다. 258

책임과 관련하여 해결해야 할 주요 질문(개인 정보 보호법에서 여전히 문제가 많고 과소 검토되는 문제)은 책임 조치를 구현하는 주요 책임이 어디에 있어야 하는지입니다. 예를 들어, 조직은 자체 감사를 수행해야 합니까? 정부 규제 기관이 감사를 수행해야 합니까? 독립적인 제3자가 감사를 수행해야 합니까?

많은 개인 정보 보호법에서는 대부분의 책임 및 거버넌스 메커니즘 구현에 대한 책임을 회사에 위임합니다. Ari Waldman 교수는 이러한 접근 방식이 비참할 정도로 비효율적이라고 비난합니다. "투명성, 영향 평가, 문서 추적 및 이들이 지원하는 전통적인 책임 메커니즘은 알고리즘 의사 결정의 토대를 마련할 뿐만 아니라 편견, 오류 및 피해에도 불구하고 확산을 좋은 것으로 간주합니다."259 Waldman은 준수 모델 대신 "독립적인 학술 전문가의 지원을 받는 규제 기관은 알고리즘 의사 결정 코드의 준수 여부를 감사해야 합니다"라고 제안합니다. 사회적 가치를 위해."260

감사 및 검토에는 실질적이고 독립적인 구성요소가 있어야 합니다.
그렇지 않으면 조직은 위험을 무시한 대가가 높을 때 제지하기 위해 애쓰게 될 것입니다. 규제는 세세한 관리를 피하고 조직이 수행할 수 있는 모든 것에 대해 허가를 요구하면서 스스로 관리하기 위해 지나치게 신뢰하는 조직 사이의 줄타기 균형을 맞춰야 합니다. 궁극적으로 내부 및 외부 책임 메커니즘이 혼합되어 있어야 합니다.

조직은 자신이 초래한 피해와 위험에 대해 의미 있는 결과에 직면해야 합니다. 그렇게 하지 않는 경우가 너무 많아 법적인 의무를 진지하게 받아들이지 않는 유인을 만들어냅니다.

5. 집행 및 구제

AI는 개인정보 보호법을 위반할 경우 구제책을 제시합니다. 데이터를 부적절하게 수집해 AI 알고리즘을 만들면 알고리즘에서 데이터를 풀어내기가 어려워진다. 알고리즘은 이미 데이터로부터 "학습"했습니다. Tiffany Li는 이 효과를 "알고리즘 그림자"라고 부릅니다.

---

257 Talia B. Gillis 및 Josh Simons, 설명 < 정당성: GDPR과 개인정보 보호의 위험성, Pa. JL & Innovation(2019).
258 ID.
259 Ari Ezra Waldman, 전력, 프로세스 및 자동화된 의사결정, 88 Fordham L. Rev. 613(2019).

260 ID.

기계 학습 모델에 입력된 데이터의 각인입니다."261 따라서 데이터 삭제 해결 방법은 "알고리즘의 그림자를 제거"하는 데 실패합니다. 즉, "이미 훈련된 모델에는 영향을 미치지 않습니다." 262 그 결과 불법적인 데이터 수집을 피할 유인이 부족해졌습니다. 이점은 알고리즘에 반영되므로 기업은 자신이 훔친 데이터를 삭제해야 하는 경우에도 앞서 나갑니다.

점점 더 많이 사용되고 있는 해결책 중 하나는 알고리즘 파괴입니다. 예를 들어, In re Everalbum, Inc. 에서 FTC는 회사에 부적절하게 수집한 데이터로 개발된 "모든 모델 또는 알고리즘"을 삭제하도록 명령했습니다.263
그러나 Li는 알고리즘 파괴의 해결책이 너무 심각할 수 있으며 "소규모 스타트업에 해를 끼치고 기술 산업의 새로운 시장 진입을 방해"할 수 있다고 주장합니다. 264 게다가 공정위가 작은 회사에 알고리즘 삭제를 명령하는 것도 하나의 일인데 Open AI 같은 거대 회사는 어떨까? FTC나 규제 당국이 수십억 달러 가치를 지닌 매우 인기 있는 알고리즘의 삭제를 명령하는 것은 상상하기 어렵습니다.

또한, 일부 데이터만 부적절하게 수집된 경우에도 이 해결 방법이 실행 가능합니까? 한 사람의 데이터가 부적절하게 포함되었다는 이유로 전체 AI 시스템을 삭제하는 것은 과잉일 것입니다. 그럼에도 불구하고, 대부분의 데이터가 부적절하게 수집되었거나 알고리즘이 상당한 피해를 입히고 있는 경우에는 알고리즘에 의한 파괴가 적절한 구제 수단이 될 수 있습니다.

또 다른 과제는 AI에 대한 자금과 투자가 엄청나게 크다는 것입니다.
성공적인 AI 도구를 개발하면 엄청난 부를 얻게 됩니다. 벌금과 집행만으로는 그러한 이익을 상쇄하기에 충분하지 않습니다. 그 결과 기업이 법을 위반하여 지름길을 택하고 큰 보물을 보상받고 나중에 사과하고 이익의 작은 부분을 갚을 수 있는 왜곡된 인센티브가 발생합니다. AI 기업가들은 허락보다 용서를 구하는 것이 낫다는 격언을 알고 있습니다.265

궁극적으로 AI에 대한 집행은 상당한 도전이 될 것입니다. "빠르게 움직여서 일을 깨뜨리는" 인센티브는 상당히 높을 것입니다. 집행자가 너무 강해지면 그러한 인센티브를 극복할 수 있는 페널티를 발행하는 경우는 거의 없습니다.

---

261 Tiffany C. Li, 알고리즘 파괴, 75 SMU L. Rev. 479, 482(2022).

262 ID. 498에서.

263 주식회사 에버앨범의 경우 (2022).

264 Li, 알고리즘 파괴, 각주 X, at 505.

265 이 격언에 대한 자세한 내용은 Fred Shapiro, Quotes Uncovered: Forgiveness, Permission, and Awesomeness, Freakonomics Blog(2010년 6월), 24, https://freakonomics.com/2010/06/quotes-uncovered-forgiveness-permission-을 참조하십시오. 그리고-굉장함/.

결론

그럼에도 불구하고 우리는 시간의 흐름을 멈출 수 없고,
우리가 만드는 기술의 발전을 멈출 수 없습니다. 우리는
삶을 숭고하게 유지하는 방법을 찾아야 하며, 프라이버시가
침해되지 않도록 해야 합니다.

– 채팅GPT

AI는 여러 방식으로 개인 정보 보호에 영향을 미치지만, 기존 문제를 리믹스하고 증폭시키는 것만큼 근본적으로 새로운 문제를 일으키지는 않는 방식인 경우가 많습니다. 개인정보 보호 측면에서 AI의 과제는 예상치 못한 일이 아닙니다. 그것은 오랫동안 예측된 미래를 향한 길을 따라가는 단계입니다.

현재의 개인 정보 보호법은 AI의 개인 정보 보호 문제를 해결하는 데 턱없이 부족합니다. AI는 개인 정보 보호법의 가장 취약한 부분에 압력을 가합니다. 개인 정보 보호법의 잘못된 접근 방식과 기타 수정되지 않은 결함은 특히 AI에 적합하지 않습니다.

개인 정보 보호법의 실질적인 개혁은 오랫동안 지연되었습니다. 정책 입안자들은 AI에 대해 우려하고 있으며 규제에 대한 새로운 접근 방식을 고려할 수 있는 창이 열린 것으로 보입니다. 바라건대, 이는 개인정보 보호법을 새로운 방향으로 전환할 수 있는 기회를 제공할 것입니다. AI의 개인 정보 보호 문제를 적절하게 규제하려면 개인 정보 보호법의 오랜 어려움과 잘못된 접근 방식을 해결해야 합니다.