The Evolution of Risk in EU Data Law

Dr. Felix Bieker

Office of the Data Protection Commissioner
of Schleswig-Holstein

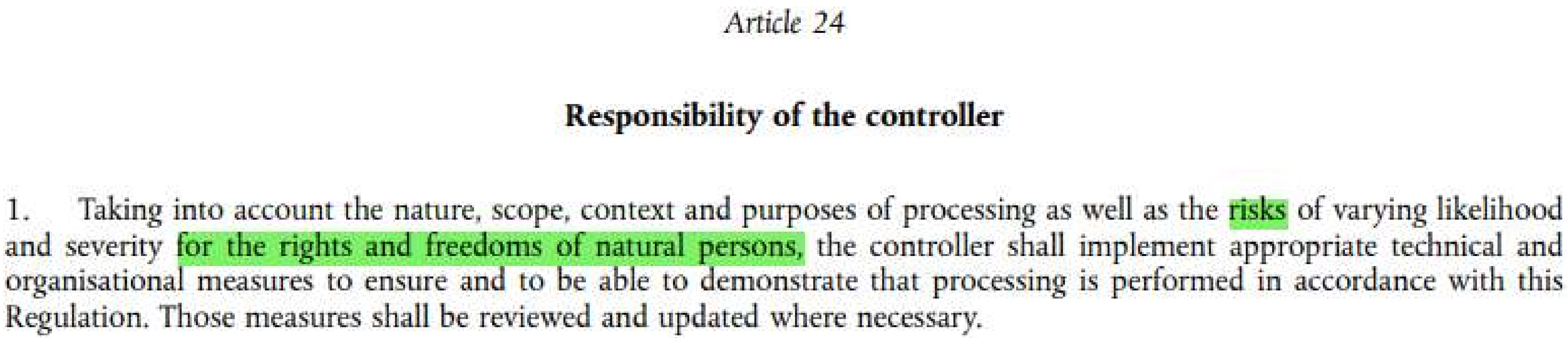
CIF Seminars, KU Leuven, 18 November 2024

Plattform Privatheit

ULD

Unabhängiges Landeszentrum für
Datenschutz Schleswig-Holstein

Risk in the GDPR

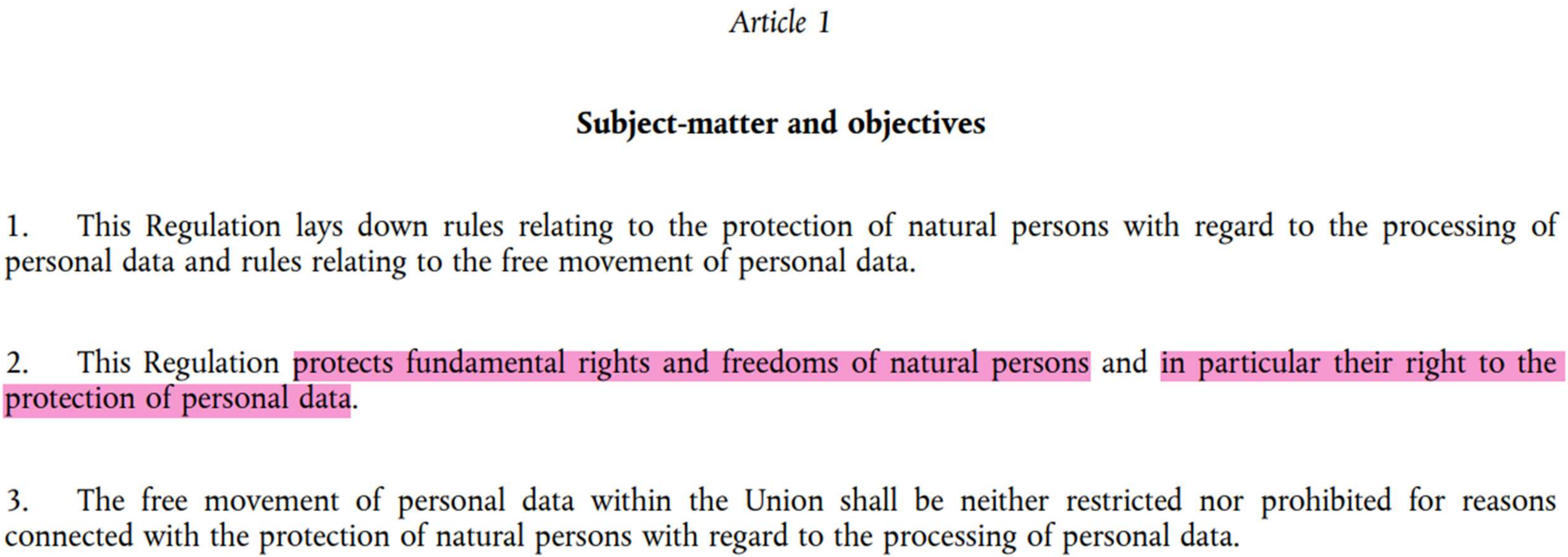


Article 24

Responsibility of the controller

1. Taking into account the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons, the controller shall implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation. Those measures shall be reviewed and updated where necessary.

Risk in the GDPR



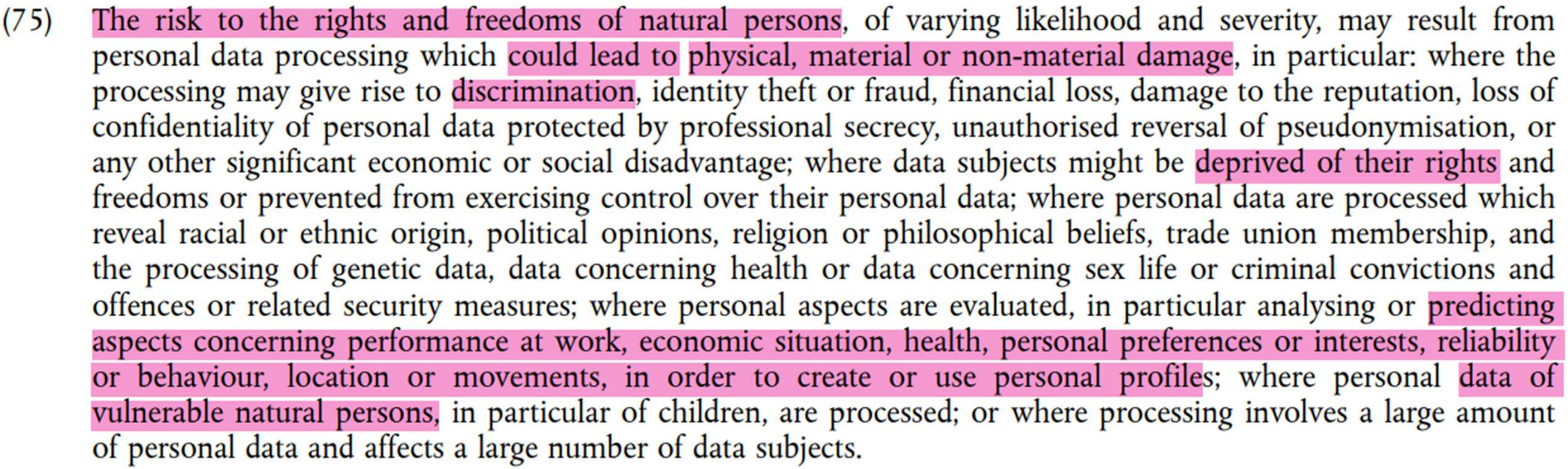
Article 1

Subject-matter and objectives

1. This Regulation lays down rules relating to the protection of natural persons with regard to the processing of personal data and rules relating to the free movement of personal data.

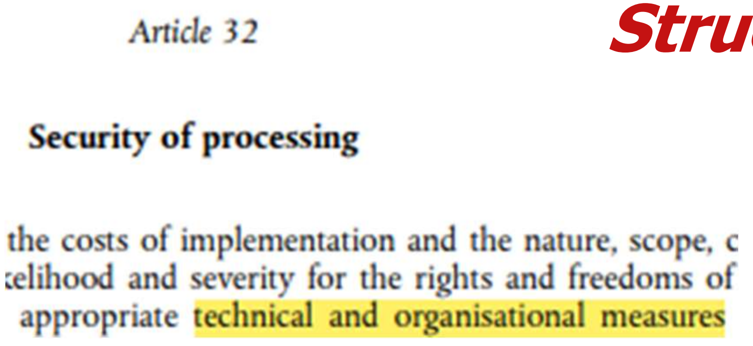
2. This Regulation protects fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data.

3. The free movement of personal data within the Union shall be neither restricted nor prohibited for reasons connected with the protection of natural persons with regard to the processing of personal data.



(75) The risk to the rights and freedoms of natural persons, of varying likelihood and severity, may result from personal data processing which could lead to physical, material or non-material damage, in particular: where the processing may give rise to discrimination, identity theft or fraud, financial loss, damage to the reputation, loss of confidentiality of personal data protected by professional secrecy, unauthorised reversal of pseudonymisation, or any other significant economic or social disadvantage; where data subjects might be deprived of their rights and freedoms or prevented from exercising control over their personal data; where personal data are processed which reveal racial or ethnic origin, political opinions, religion or philosophical beliefs, trade union membership, and the processing of genetic data, data concerning health or data concerning sex life or criminal convictions and offences or related security measures; where personal aspects are evaluated, in particular analysing or predicting aspects concerning performance at work, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements, in order to create or use personal profiles; where personal data of vulnerable natural persons, in particular of children, are processed; or where processing involves a large amount of personal data and affects a large number of data subjects.

Structural Data Protection

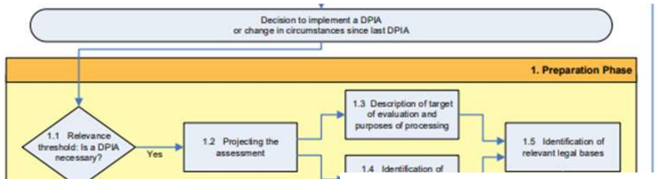


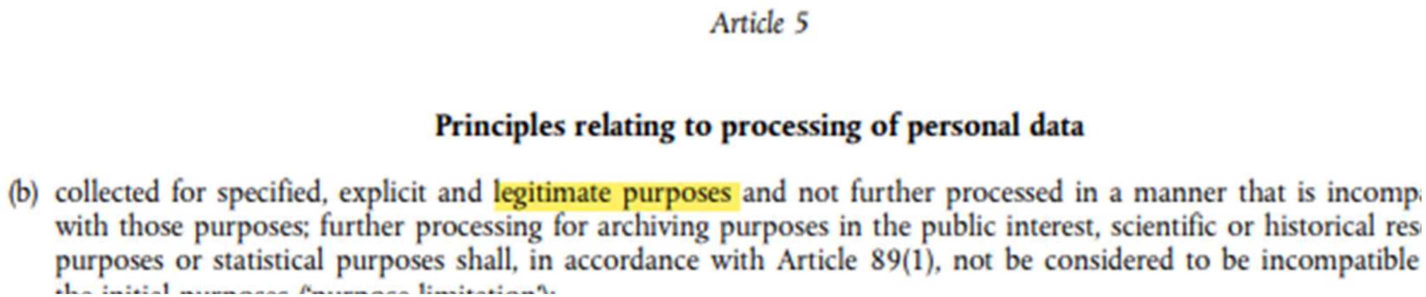
Article 32

Security of processing

the costs of implementation and the nature, scope, c
ælihood and severity for the rights and freedoms of
appropriate technical and organisational measures

DPIA

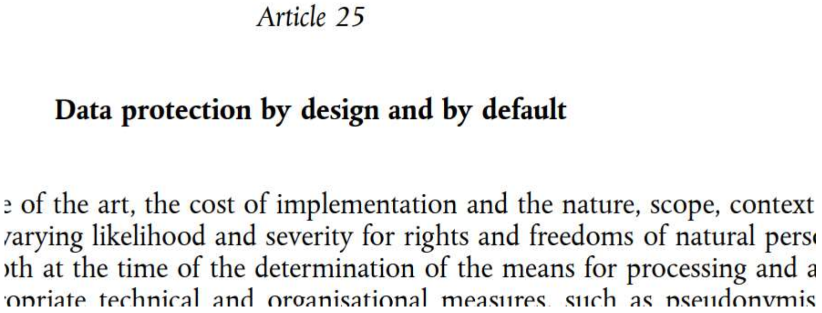

Decision to implement a DPIA
or change in circumstances since last DPIA
1. Preparation Phase
1.1 Relevance threshold: Is a DPIA necessary?
Yes
No
(Documentation
1.2 Projecting the assessment
1.3 Description of target of evaluation and purposes of processing
1.4 Identification of
1.5 Identification of relevant legal bases



Article 5

Principles relating to processing of personal data

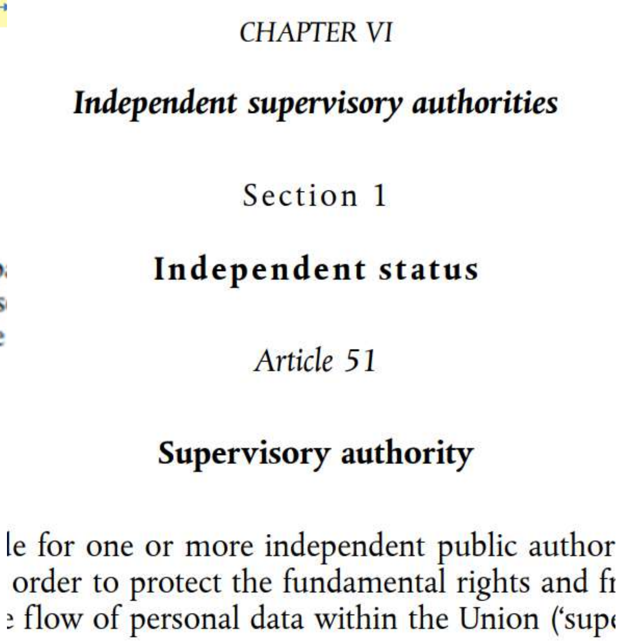
(b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incomp
with those purposes; further processing for archiving purposes in the public interest, scientific or historical res
purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible
the initial purposes ('purpose limitation');



Article 25

Data protection by design and by default

ɛ of the art, the cost of implementation and the nature, scope, context
varying likelihood and severity for rights and freedoms of natural pers
oth at the time of the determination of the means for processing and a
opriate technical and organisational measures, such as pseudonymis



CHAPTER VI

Independent supervisory authorities

Section 1

Independent status

Article 51

Supervisory authority

le for one or more independent public author
order to protect the fundamental rights and fı
ɛ flow of personal data within the Union ('sup

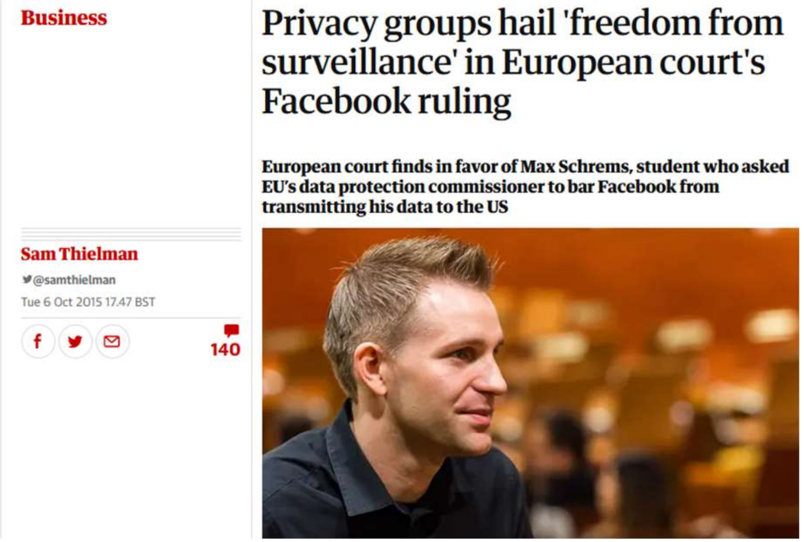
Individual Data Protection

CHAPTER III

Rights of the data subject

Article 7

Conditions for consent



Business

Privacy groups hail 'freedom from surveillance' in European court's Facebook ruling

European court finds in favor of Max Schrems, student who asked EU's data protection commissioner to bar Facebook from transmitting his data to the US

Sam Thielman

@samthielman

Tue 6 Oct 2015 17.47 BST

140

https://www.theguardian.com/business/2015/oct/06/europe-court-right-to-privacy-max-schrems-us-tech-companies

Privacy Enhancing Technologies
protect your online privacy
enisa
Time to adopt PETs!
Privacy Enhancing Technologies (PETs) help to protect
online privacy following the simple approach "reduce, protect, detect".
The future starts now: make it a habit, adopt PETs.

https://www.enisa.europa.eu/media/multimedia/posters/2018time-to-adopt-pets2019-poster

Structural Data Protection

Article 32

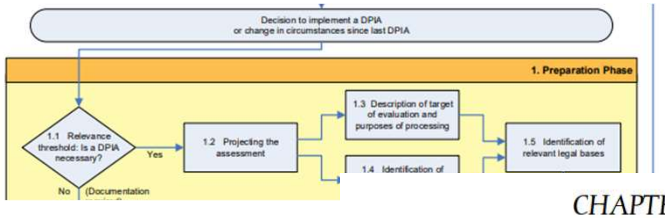
Security of processing

the costs of implementation and the nature, scope, c

elihood and severity for the rights and freedoms of

appropriate technical and organisational measures

DPIA


Decision to implement a DPIA
or change in circumstances since last DPIA
1. Preparation Phase
1.1 Relevance threshold: Is a DPIA necessary?
Yes
No
(Documentation
1.2 Projecting the assessment
1.3 Description of target of evaluation and purposes of processing
1.4 Identification of
1.5 Identification of relevant legal bases

Article 5

Principles relating to processing of personal data

(b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incomp
with those purposes; further processing for archiving purposes in the public interest, scientific or historical res
purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible
the initial purposes ('purpose limitation');

CHAPTER VI

Independent supervisory authorities

Section 1

Independent status

Article 51

Supervisory authority

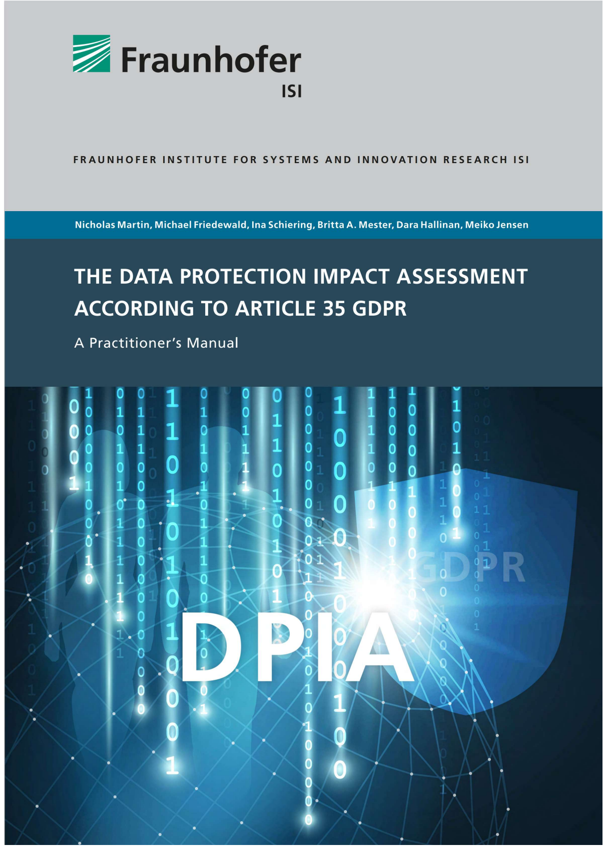
le for one or more independent public author
order to protect the fundamental rights and fı
flow of personal data within the Union ('supe

Article 25

Data protection by design and by default

of the art, the cost of implementation and the nature, scope, context
varying likelihood and severity for rights and freedoms of natural pers
oth at the time of the determination of the means for processing and a
opriate technical and organisational measures, such as pseudonymis

Process for DPIA



Fraunhofer
ISI

FRAUNHOFER INSTITUTE FOR SYSTEMS AND INNOVATION RESEARCH ISI

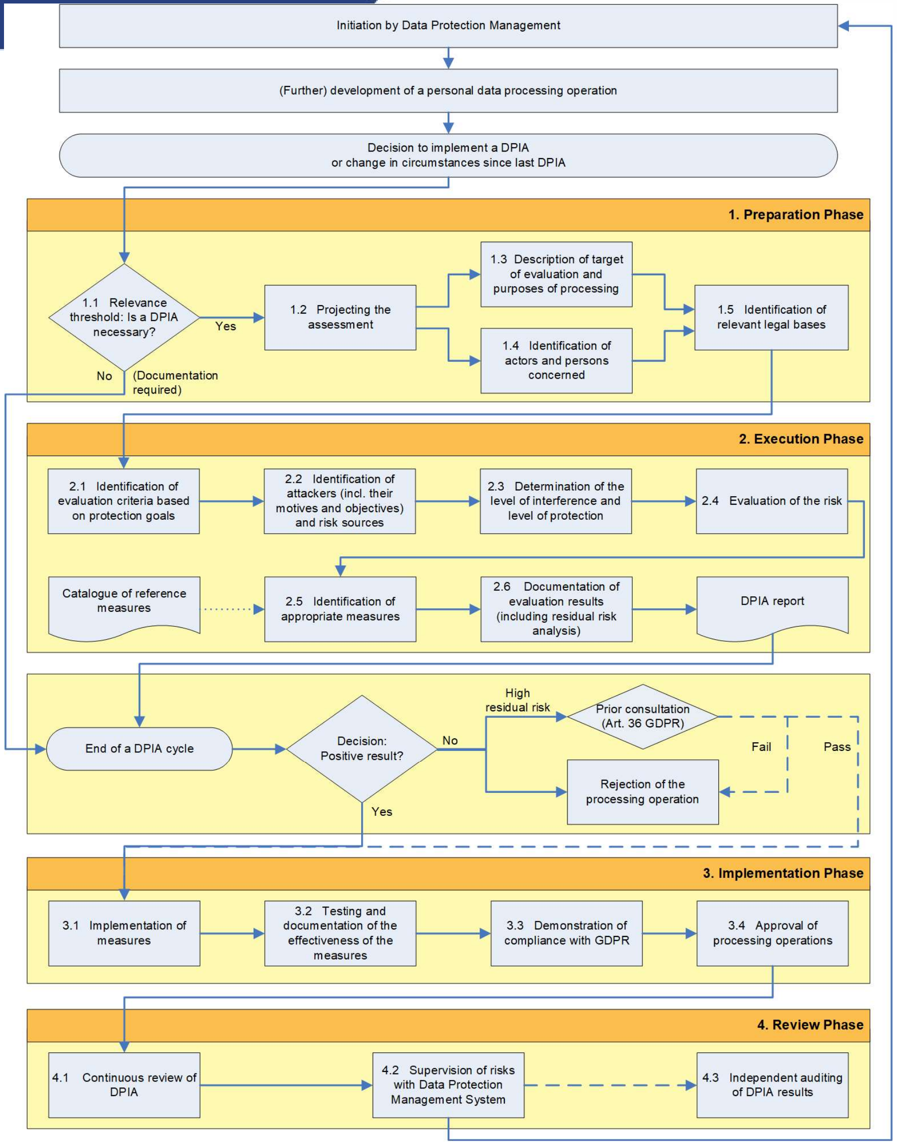
Nicholas Martin, Michael Friedewald, Ina Schiering, Britta A. Mester, Dara Hallinan, Meiko Jensen

THE DATA PROTECTION IMPACT ASSESSMENT ACCORDING TO ARTICLE 35 GDPR

A Practitioner's Manual

https://publica.fraunhofer.de/entities/publication/a56af9f6-94e9-438b-9605-0d1d85f5aaf4

Plattform Privatheit



Initiation by Data Protection Management

(Further) development of a personal data processing operation

Decision to implement a DPIA or change in circumstances since last DPIA

1. Preparation Phase

1.1 Relevance threshold: Is a DPIA necessary?

Yes

No (Documentation required)

1.2 Projecting the assessment

1.3 Description of target of evaluation and purposes of processing

1.4 Identification of actors and persons concerned

1.5 Identification of relevant legal bases

2. Execution Phase

2.1 Identification of evaluation criteria based on protection goals

2.2 Identification of attackers (incl. their motives and objectives) and risk sources

2.3 Determination of the level of interference and level of protection

2.4 Evaluation of the risk

Catalogue of reference measures

2.5 Identification of appropriate measures

2.6 Documentation of evaluation results (including residual risk analysis)

DPIA report

End of a DPIA cycle

Decision: Positive result?

No

High residual risk

Prior consultation (Art. 36 GDPR)

Fail

Pass

Rejection of the processing operation

Yes

3. Implementation Phase

3.1 Implementation of measures

3.2 Testing and documentation of the effectiveness of the measures

3.3 Demonstration of compliance with GDPR

3.4 Approval of processing operations

4. Review Phase

4.1 Continuous review of DPIA

4.2 Supervision of risks with Data Protection Management System

4.3 Independent auditing of DPIA results

DECEIVED BY DESIGN

How tech companies use dark patterns to discourage us from exercising our rights to privacy

27.06.2018

FORBRUKERRÅDET

Information Commissioner's Office

Democracy disrupted?

Personal information and political influence

11 July 2018

ico.

Information Commissioner's Office

HUMAN RIGHTS WATCH

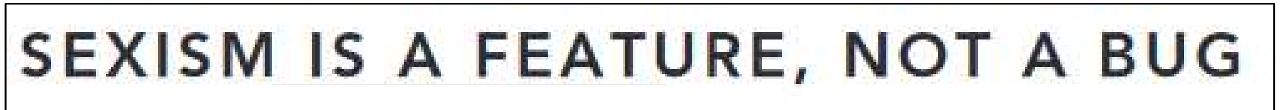
"All This Terror Because of a Photo"

Digital Targeting and Its Offline Consequences for LGBT People in the Middle East and North Africa

THE SOCIAL ATROCITY

META AND THE RIGHT TO REMEDY FOR THE ROHINGYA

AMNESTY INTERNATIONAL



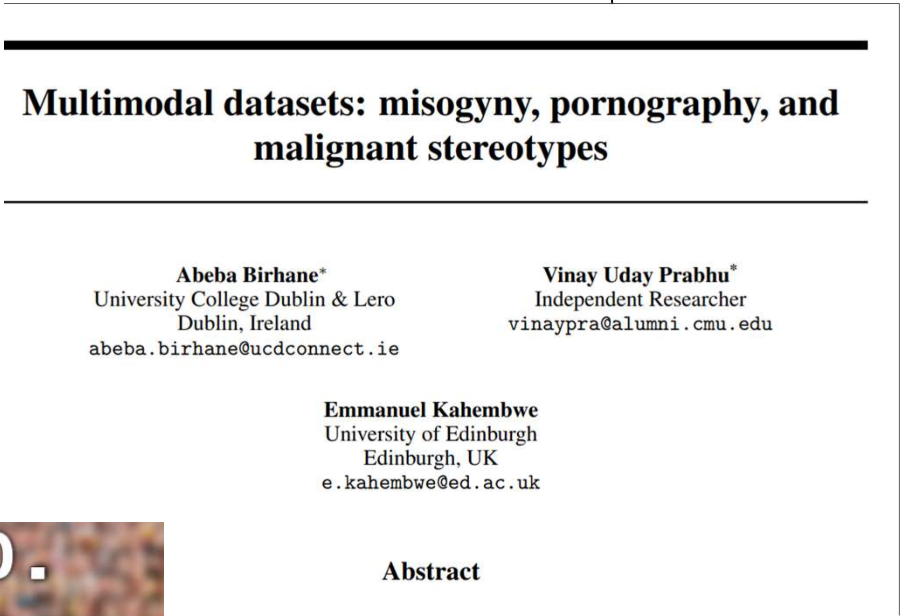
SEXISM IS A FEATURE, NOT A BUG

Mar Hicks

CODED INJUSTICE

SURVEILLANCE AND DISCRIMINATION IN DENMARK'S AUTOMATED WELFARE STATE

AMNESTY INTERNATIONAL



Multimodal datasets: misogyny, pornography, and malignant stereotypes

Abeba Birhane*
University College Dublin & Lero
Dublin, Ireland
abeba.birhane@ucdconnect.ie

Vinay Uday Prabhu*
Independent Researcher
vinaypra@alumni.cmu.edu

Emmanuel Kahembwe
University of Edinburgh
Edinburgh, UK
e.kahembwe@ed.ac.uk

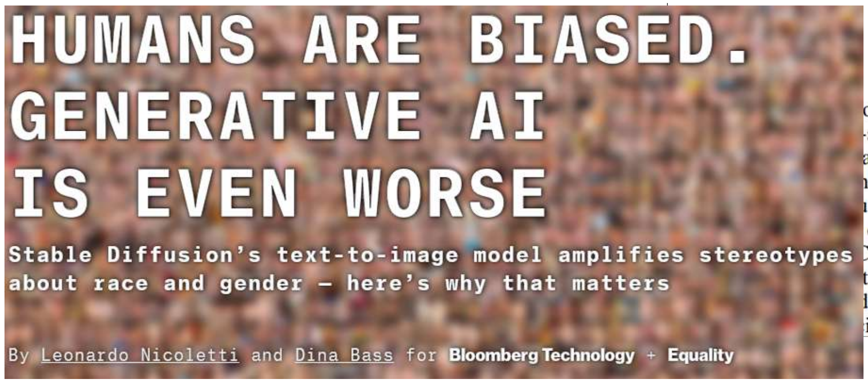
Abstract

ow entered tl
-sized datase
as given rise
hile generatin
is curation p
data availab
Crawl dataset
trenched bias
del) trained
ific calls of

More than a Glitch

< Confronting Race, >
< Gender, >
< and Ability Bias >
< in Tech >

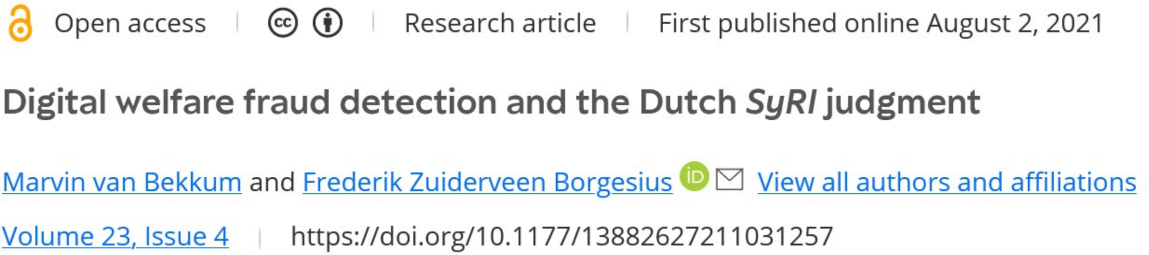
Meredith Broussard



HUMANS ARE BIASED. GENERATIVE AI IS EVEN WORSE

Stable Diffusion's text-to-image model amplifies stereotypes about race and gender — here's why that matters

By Leonardo Nicoletti and Dina Bass for Bloomberg Technology + Equality



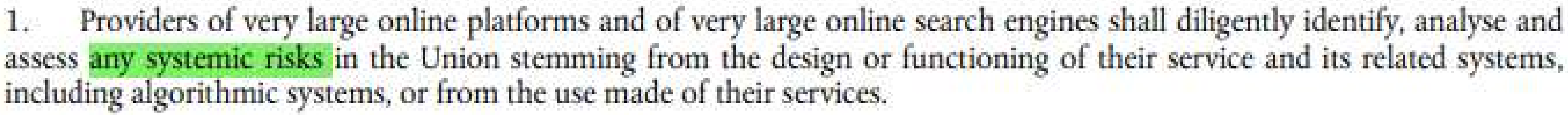
Open access | Research article | First published online August 2, 2021

Digital welfare fraud detection and the Dutch *SyRI* judgment

Marvin van Bekkum and Frederik Zuiderveen Borgesius View all authors and affiliations

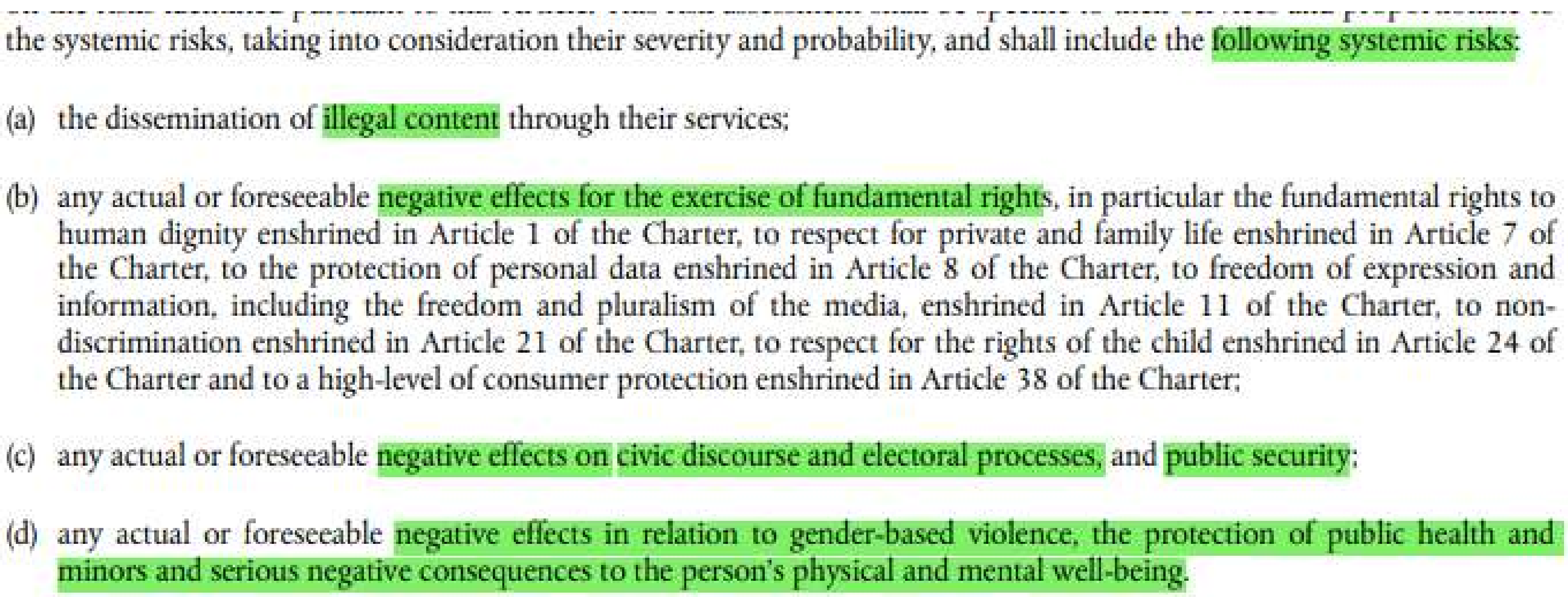
Volume 23, Issue 4 | https://doi.org/10.1177/13882627211031257

Risk in the DSA



1. Providers of very large online platforms and of very large online search engines shall diligently identify, analyse and assess any systemic risks in the Union stemming from the design or functioning of their service and its related systems, including algorithmic systems, or from the use made of their services.

Risk in the DSA



the systemic risks, taking into consideration their severity and probability, and shall include the following systemic risks:

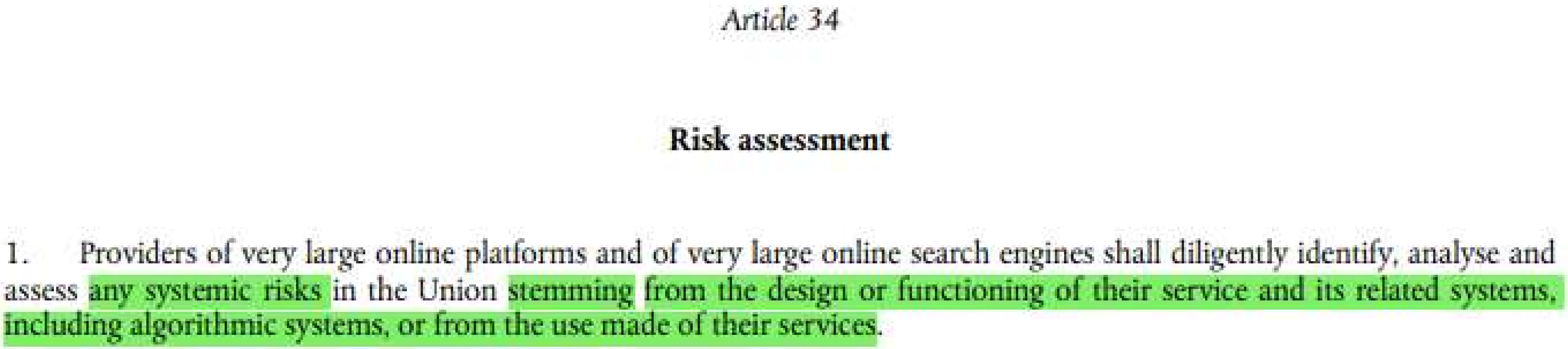
(a) the dissemination of illegal content through their services;

(b) any actual or foreseeable negative effects for the exercise of fundamental rights, in particular the fundamental rights to human dignity enshrined in Article 1 of the Charter, to respect for private and family life enshrined in Article 7 of the Charter, to the protection of personal data enshrined in Article 8 of the Charter, to freedom of expression and information, including the freedom and pluralism of the media, enshrined in Article 11 of the Charter, to non-discrimination enshrined in Article 21 of the Charter, to respect for the rights of the child enshrined in Article 24 of the Charter and to a high-level of consumer protection enshrined in Article 38 of the Charter;

(c) any actual or foreseeable negative effects on civic discourse and electoral processes, and public security;

(d) any actual or foreseeable negative effects in relation to gender-based violence, the protection of public health and minors and serious negative consequences to the person's physical and mental well-being.

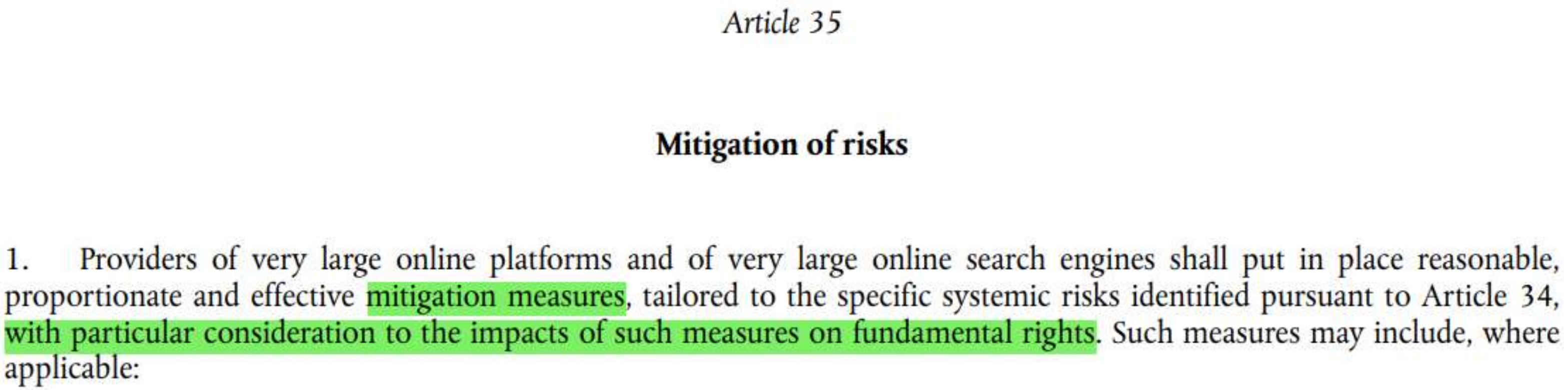
Risk Assessment in the DSA



Article 34

Risk assessment

1. Providers of very large online platforms and of very large online search engines shall diligently identify, analyse and assess any systemic risks in the Union stemming from the design or functioning of their service and its related systems, including algorithmic systems, or from the use made of their services.

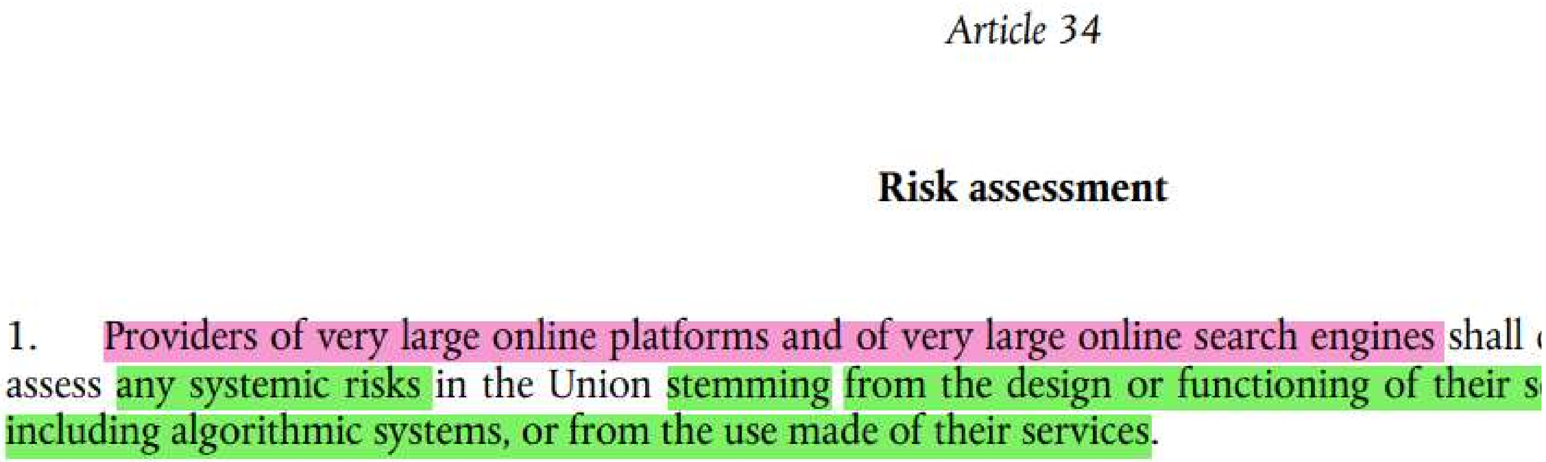


Article 35

Mitigation of risks

1. Providers of very large online platforms and of very large online search engines shall put in place reasonable, proportionate and effective mitigation measures, tailored to the specific systemic risks identified pursuant to Article 34, with particular consideration to the impacts of such measures on fundamental rights. Such measures may include, where applicable:

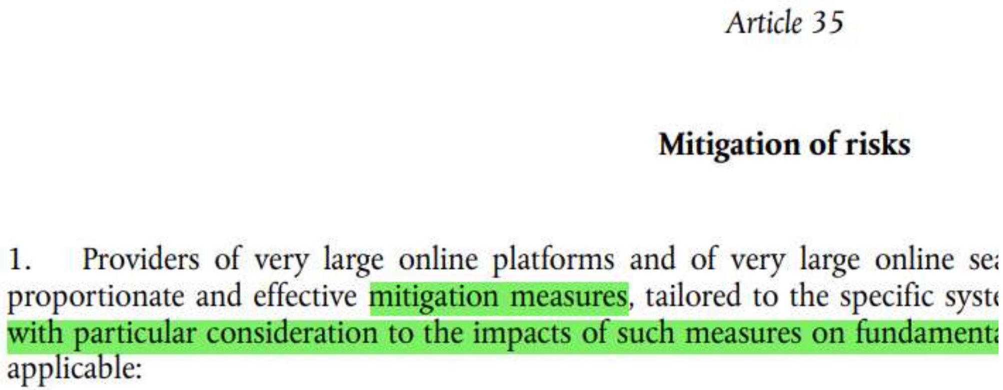
Risk Assessment in the DSA



Article 34

Risk assessment

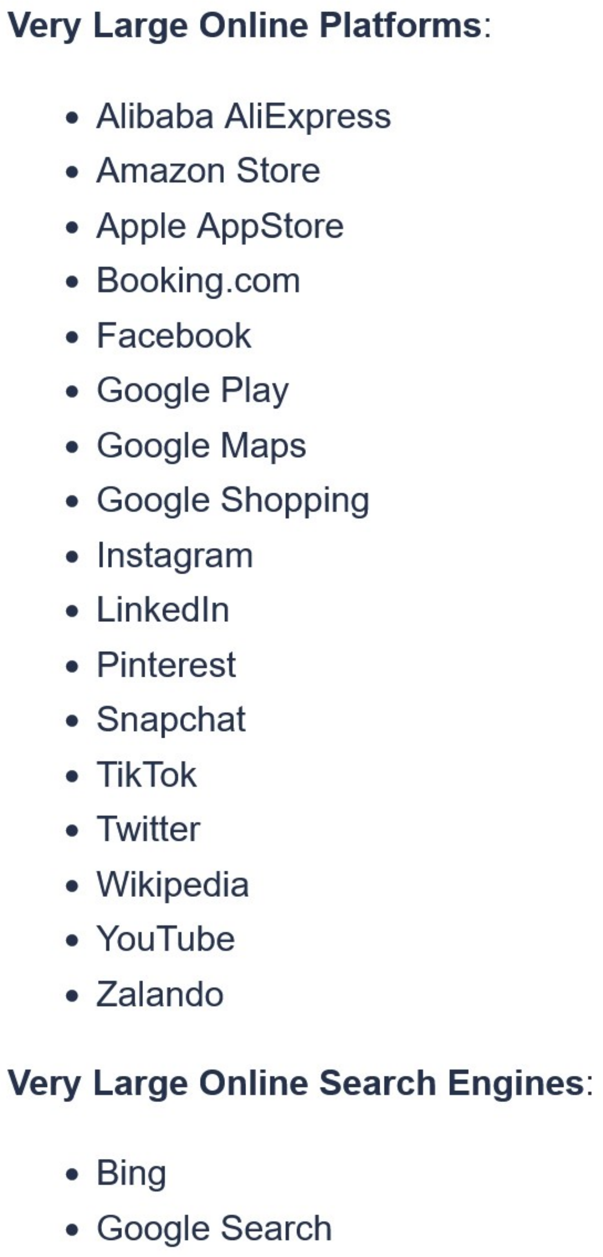
1. Providers of very large online platforms and of very large online search engines shall d assess any systemic risks in the Union stemming from the design or functioning of their s including algorithmic systems, or from the use made of their services.



Article 35

Mitigation of risks

1. Providers of very large online platforms and of very large online sea proportionate and effective mitigation measures, tailored to the specific syste with particular consideration to the impacts of such measures on fundamenta applicable:



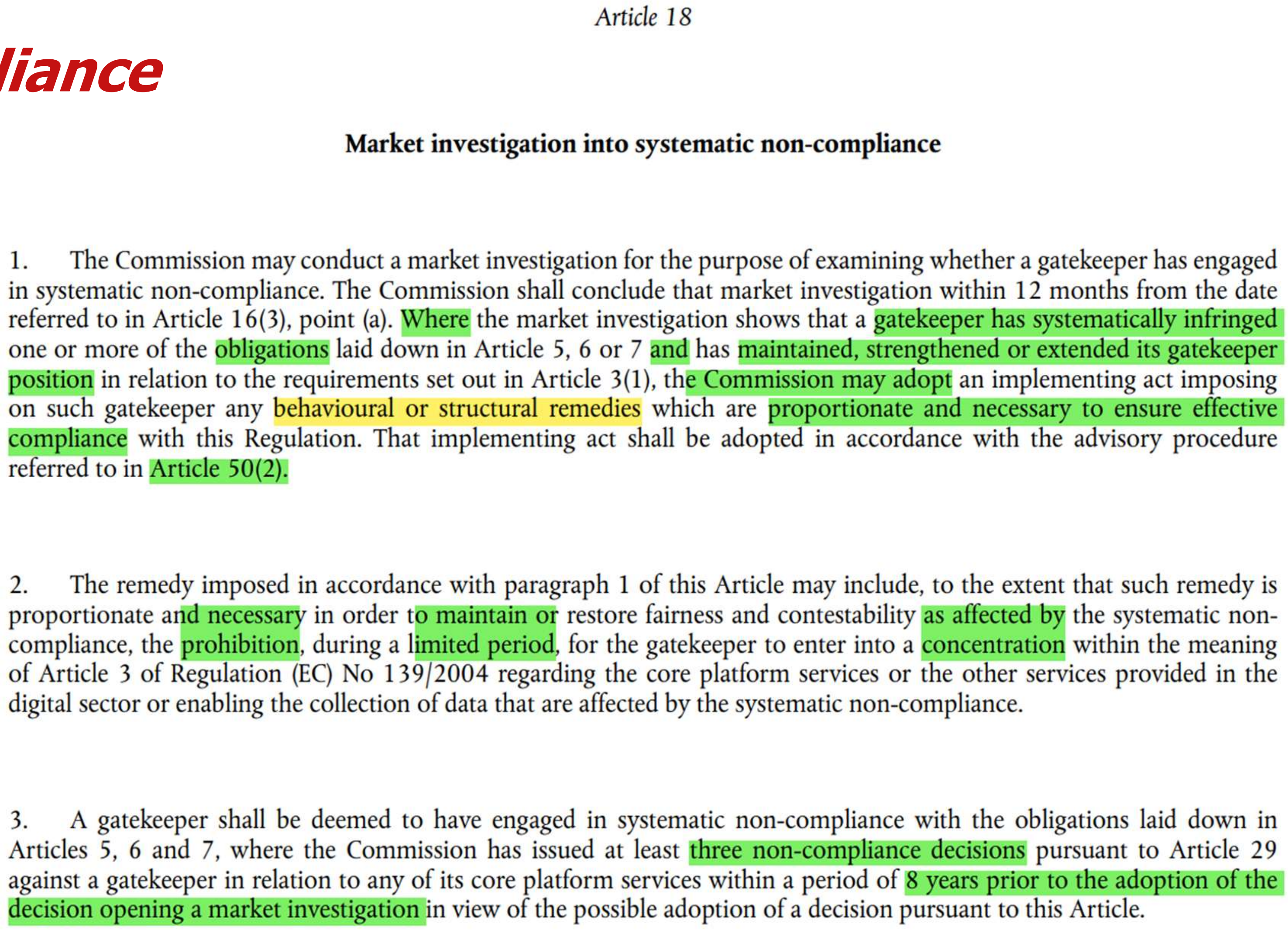
Very Large Online Platforms:

- Alibaba AliExpress
- Amazon Store
- Apple AppStore
- Booking.com
- Facebook
- Google Play
- Google Maps
- Google Shopping
- Instagram
- LinkedIn
- Pinterest
- Snapchat
- TikTok
- Twitter
- Wikipedia
- YouTube
- Zalando

Very Large Online Search Engines:

- Bing
- Google Search

Systemic Non-Compliance



Article 18

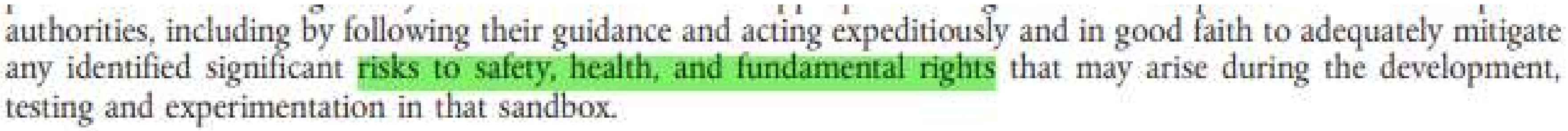
Market investigation into systematic non-compliance

1. The Commission may conduct a market investigation for the purpose of examining whether a gatekeeper has engaged in systematic non-compliance. The Commission shall conclude that market investigation within 12 months from the date referred to in Article 16(3), point (a). Where the market investigation shows that a gatekeeper has systematically infringed one or more of the obligations laid down in Article 5, 6 or 7 and has maintained, strengthened or extended its gatekeeper position in relation to the requirements set out in Article 3(1), the Commission may adopt an implementing act imposing on such gatekeeper any behavioural or structural remedies which are proportionate and necessary to ensure effective compliance with this Regulation. That implementing act shall be adopted in accordance with the advisory procedure referred to in Article 50(2).

2. The remedy imposed in accordance with paragraph 1 of this Article may include, to the extent that such remedy is proportionate and necessary in order to maintain or restore fairness and contestability as affected by the systematic non-compliance, the prohibition, during a limited period, for the gatekeeper to enter into a concentration within the meaning of Article 3 of Regulation (EC) No 139/2004 regarding the core platform services or the other services provided in the digital sector or enabling the collection of data that are affected by the systematic non-compliance.

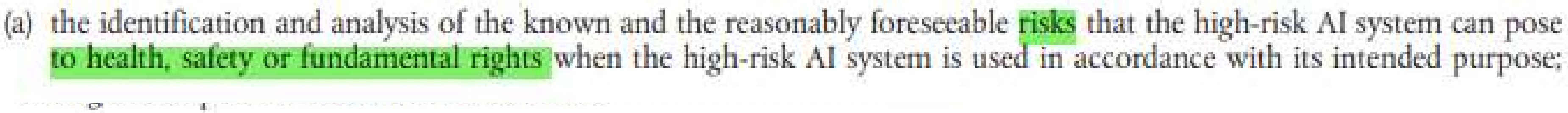
3. A gatekeeper shall be deemed to have engaged in systematic non-compliance with the obligations laid down in Articles 5, 6 and 7, where the Commission has issued at least three non-compliance decisions pursuant to Article 29 against a gatekeeper in relation to any of its core platform services within a period of 8 years prior to the adoption of the decision opening a market investigation in view of the possible adoption of a decision pursuant to this Article.

Risk in the AI Act



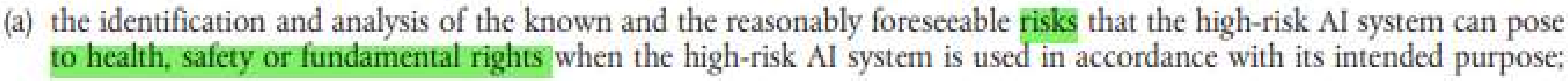
authorities, including by following their guidance and acting expeditiously and in good faith to adequately mitigate any identified significant risks to safety, health, and fundamental rights that may arise during the development, testing and experimentation in that sandbox.

Risk in the AI Act

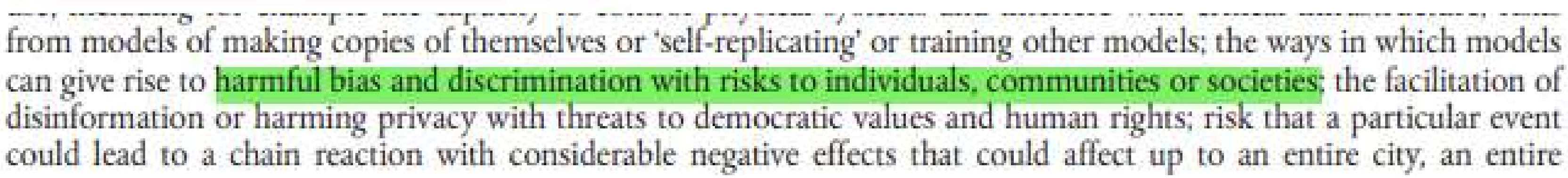


(a) the identification and analysis of the known and the reasonably foreseeable risks that the high-risk AI system can pose to health, safety or fundamental rights when the high-risk AI system is used in accordance with its intended purpose;

Risk in the AI Act

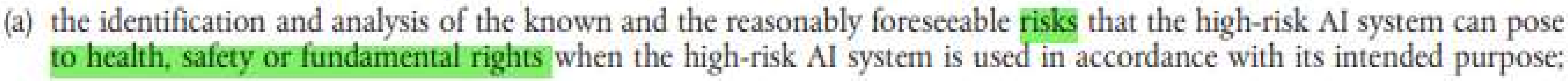


(a) the identification and analysis of the known and the reasonably foreseeable risks that the high-risk AI system can pose to health, safety or fundamental rights when the high-risk AI system is used in accordance with its intended purpose;

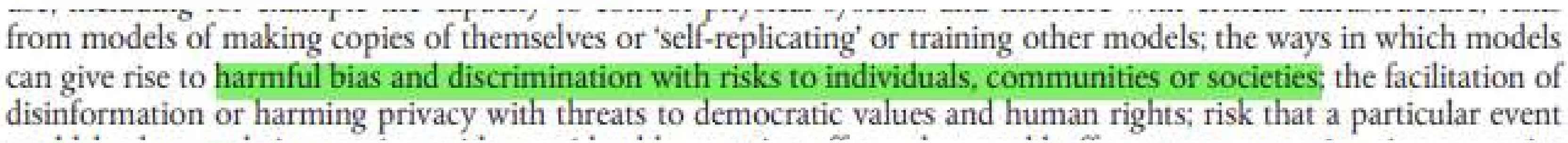


from models of making copies of themselves or 'self-replicating' or training other models; the ways in which models can give rise to harmful bias and discrimination with risks to individuals, communities or societies; the facilitation of disinformation or harming privacy with threats to democratic values and human rights; risk that a particular event could lead to a chain reaction with considerable negative effects that could affect up to an entire city, an entire

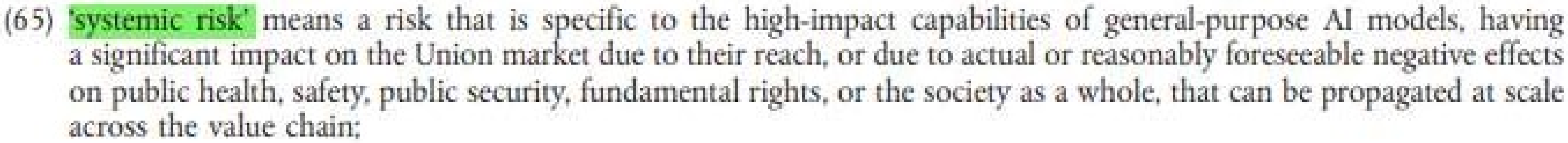
Risk in the AI Act



(a) the identification and analysis of the known and the reasonably foreseeable risks that the high-risk AI system can pose to health, safety or fundamental rights when the high-risk AI system is used in accordance with its intended purpose;

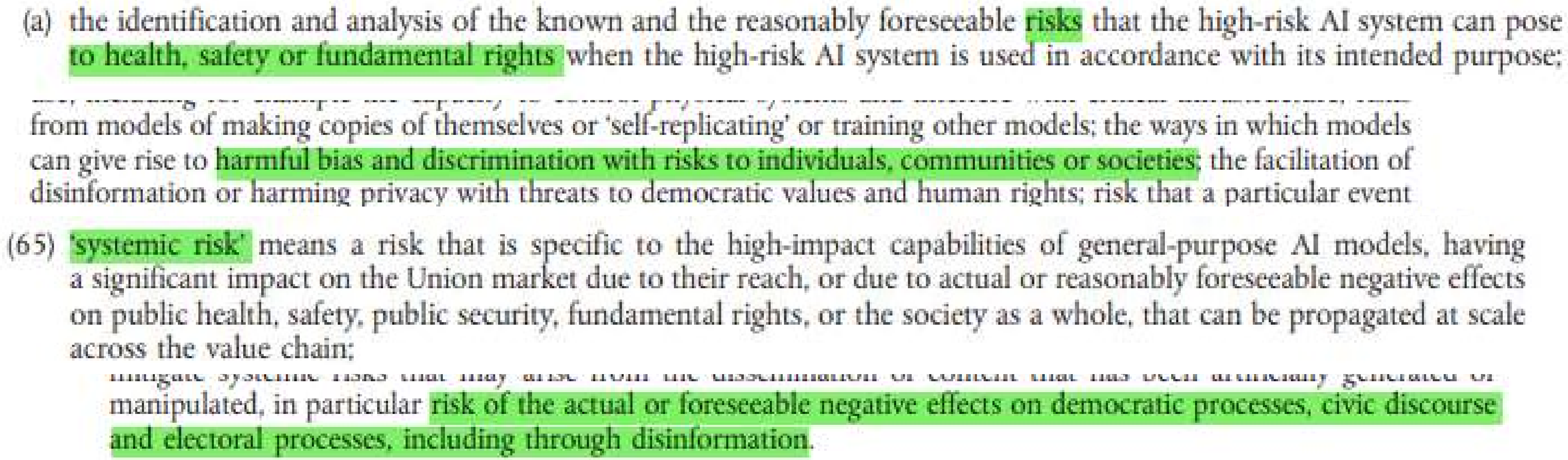


from models of making copies of themselves or 'self-replicating' or training other models; the ways in which models can give rise to harmful bias and discrimination with risks to individuals, communities or societies; the facilitation of disinformation or harming privacy with threats to democratic values and human rights; risk that a particular event



(65) 'systemic risk' means a risk that is specific to the high-impact capabilities of general-purpose AI models, having a significant impact on the Union market due to their reach, or due to actual or reasonably foreseeable negative effects on public health, safety, public security, fundamental rights, or the society as a whole, that can be propagated at scale across the value chain;

Risk in the AI Act



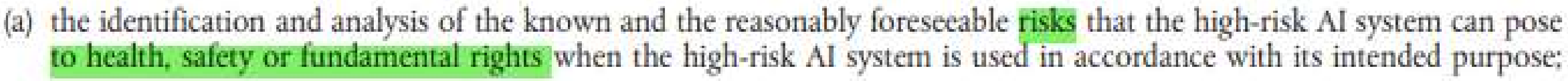
(a) the identification and analysis of the known and the reasonably foreseeable risks that the high-risk AI system can pose to health, safety or fundamental rights when the high-risk AI system is used in accordance with its intended purpose;

from models of making copies of themselves or 'self-replicating' or training other models; the ways in which models can give rise to harmful bias and discrimination with risks to individuals, communities or societies; the facilitation of disinformation or harming privacy with threats to democratic values and human rights; risk that a particular event

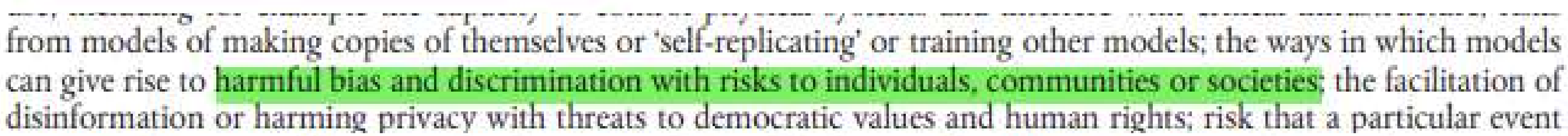
(65) 'systemic risk' means a risk that is specific to the high-impact capabilities of general-purpose AI models, having a significant impact on the Union market due to their reach, or due to actual or reasonably foreseeable negative effects on public health, safety, public security, fundamental rights, or the society as a whole, that can be propagated at scale across the value chain;

manipulated, in particular risk of the actual or foreseeable negative effects on democratic processes, civic discourse and electoral processes, including through disinformation.

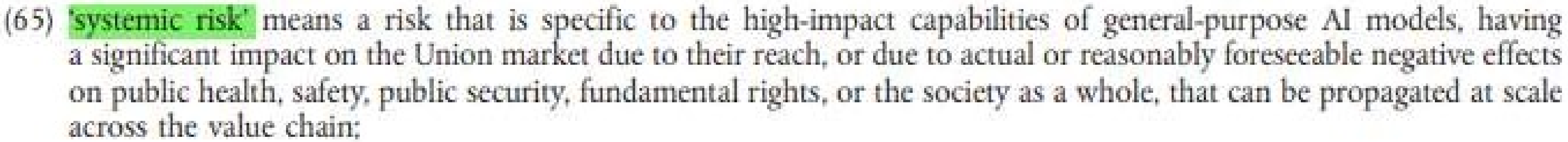
Risk in the AI Act



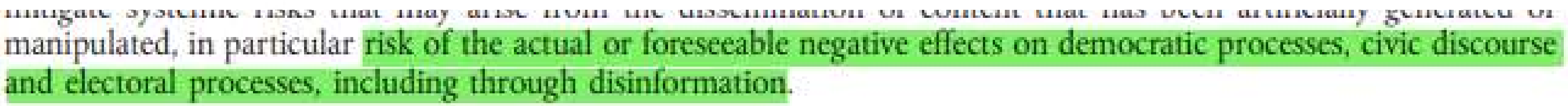
(a) the identification and analysis of the known and the reasonably foreseeable risks that the high-risk AI system can pose to health, safety or fundamental rights when the high-risk AI system is used in accordance with its intended purpose;



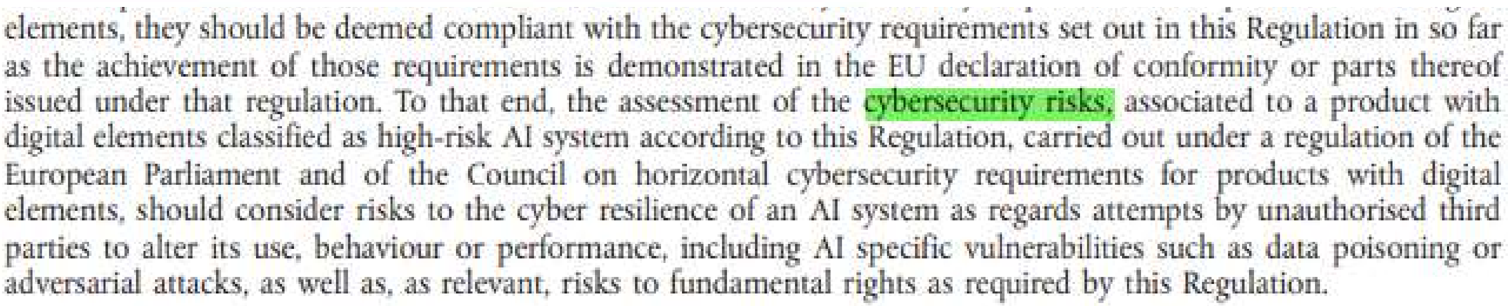
use, including for example the capacity to control physical systems and interfere with critical infrastructure; risks from models of making copies of themselves or 'self-replicating' or training other models; the ways in which models can give rise to harmful bias and discrimination with risks to individuals, communities or societies; the facilitation of disinformation or harming privacy with threats to democratic values and human rights; risk that a particular event



(65) 'systemic risk' means a risk that is specific to the high-impact capabilities of general-purpose AI models, having a significant impact on the Union market due to their reach, or due to actual or reasonably foreseeable negative effects on public health, safety, public security, fundamental rights, or the society as a whole, that can be propagated at scale across the value chain;

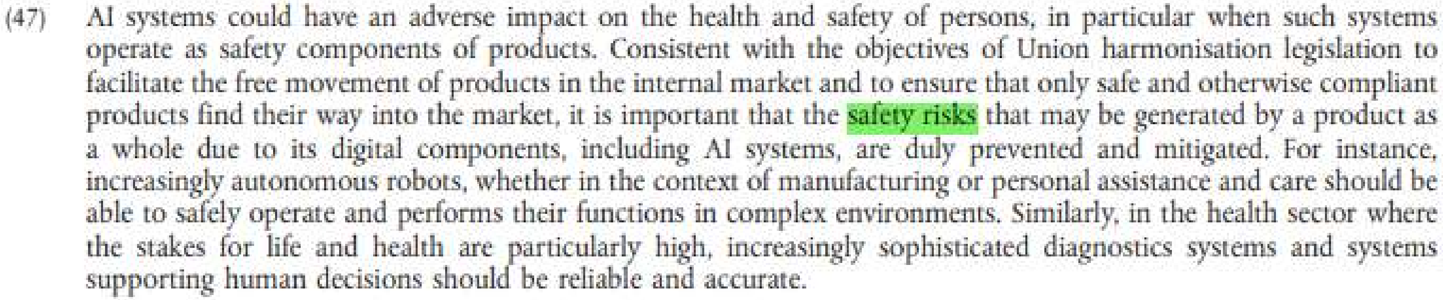


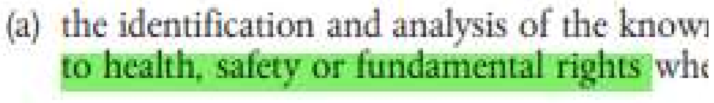
mitigate systemic risks that may arise from the dissemination of content that has been artificially generated or manipulated, in particular risk of the actual or foreseeable negative effects on democratic processes, civic discourse and electoral processes, including through disinformation.

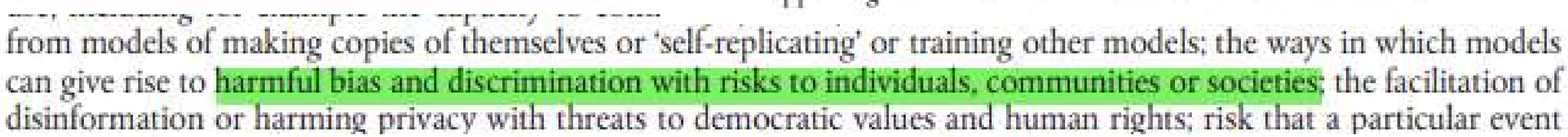


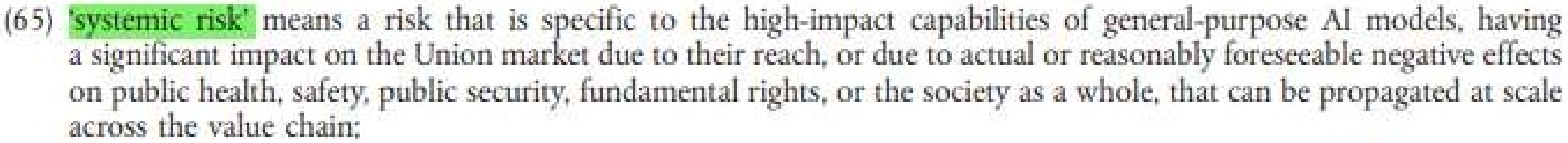
elements, they should be deemed compliant with the cybersecurity requirements set out in this Regulation in so far as the achievement of those requirements is demonstrated in the EU declaration of conformity or parts thereof issued under that regulation. To that end, the assessment of the cybersecurity risks, associated to a product with digital elements classified as high-risk AI system according to this Regulation, carried out under a regulation of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements, should consider risks to the cyber resilience of an AI system as regards attempts by unauthorised third parties to alter its use, behaviour or performance, including AI specific vulnerabilities such as data poisoning or adversarial attacks, as well as, as relevant, risks to fundamental rights as required by this Regulation.

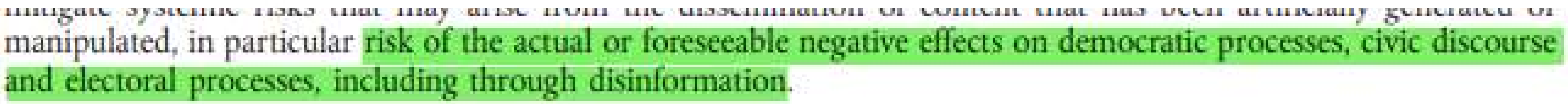
Risk in the AI Act

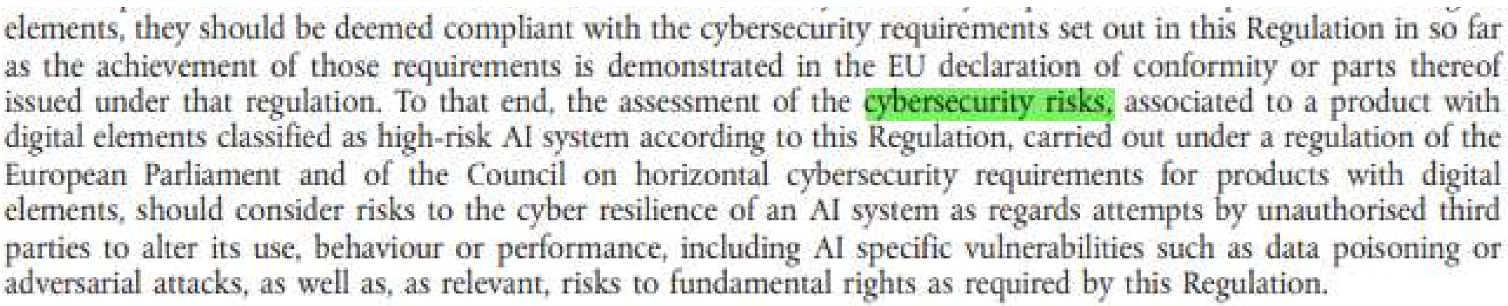

(47) AI systems could have an adverse impact on the health and safety of persons, in particular when such systems operate as safety components of products. Consistent with the objectives of Union harmonisation legislation to facilitate the free movement of products in the internal market and to ensure that only safe and otherwise compliant products find their way into the market, it is important that the safety risks that may be generated by a product as a whole due to its digital components, including AI systems, are duly prevented and mitigated. For instance, increasingly autonomous robots, whether in the context of manufacturing or personal assistance and care should be able to safely operate and performs their functions in complex environments. Similarly, in the health sector where the stakes for life and health are particularly high, increasingly sophisticated diagnostics systems and systems supporting human decisions should be reliable and accurate.


(a) the identification and analysis of the know
to health, safety or fundamental rights whe

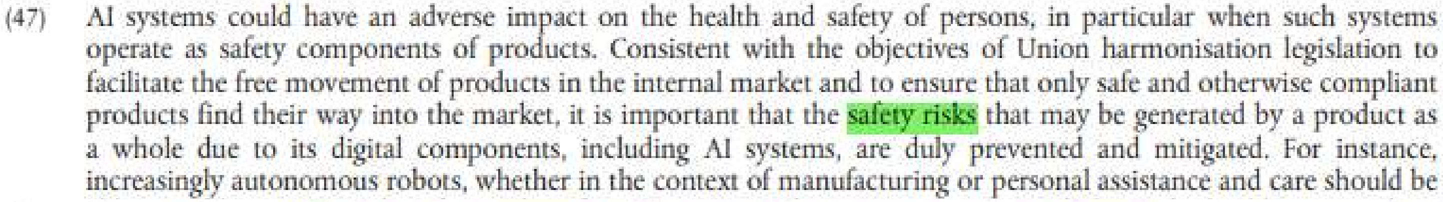

from models of making copies of themselves or 'self-replicating' or training other models; the ways in which models can give rise to harmful bias and discrimination with risks to individuals, communities or societies; the facilitation of disinformation or harming privacy with threats to democratic values and human rights; risk that a particular event


(65) 'systemic risk' means a risk that is specific to the high-impact capabilities of general-purpose AI models, having a significant impact on the Union market due to their reach, or due to actual or reasonably foreseeable negative effects on public health, safety, public security, fundamental rights, or the society as a whole, that can be propagated at scale across the value chain;

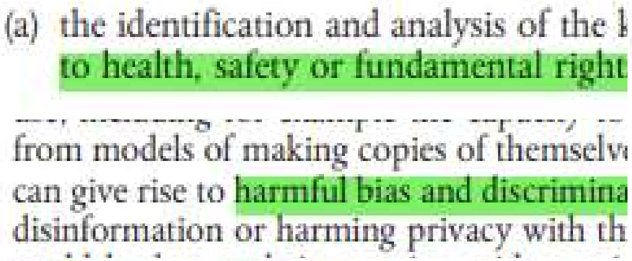

mitigate systemic risks that may arise from the dissemination of content that has been artificially generated or manipulated, in particular risk of the actual or foreseeable negative effects on democratic processes, civic discourse and electoral processes, including through disinformation.


elements, they should be deemed compliant with the cybersecurity requirements set out in this Regulation in so far as the achievement of those requirements is demonstrated in the EU declaration of conformity or parts thereof issued under that regulation. To that end, the assessment of the cybersecurity risks, associated to a product with digital elements classified as high-risk AI system according to this Regulation, carried out under a regulation of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements, should consider risks to the cyber resilience of an AI system as regards attempts by unauthorised third parties to alter its use, behaviour or performance, including AI specific vulnerabilities such as data poisoning or adversarial attacks, as well as, as relevant, risks to fundamental rights as required by this Regulation.

Risk in the AI Act

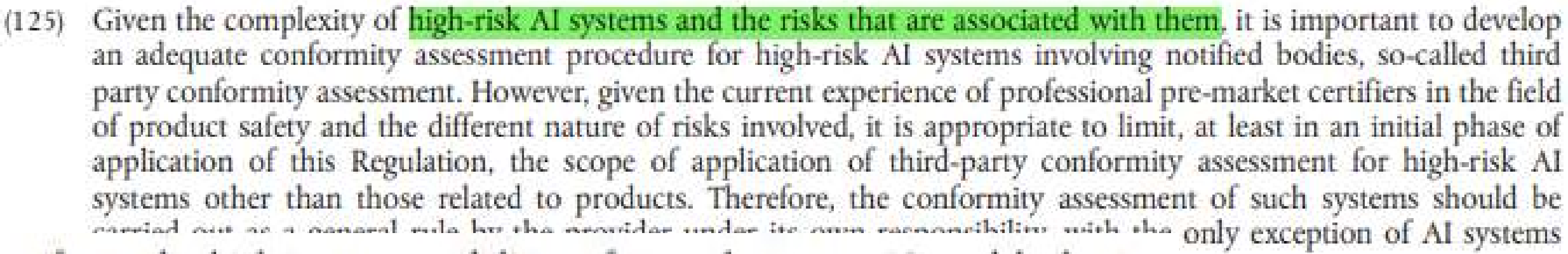


(47) AI systems could have an adverse impact on the health and safety of persons, in particular when such systems operate as safety components of products. Consistent with the objectives of Union harmonisation legislation to facilitate the free movement of products in the internal market and to ensure that only safe and otherwise compliant products find their way into the market, it is important that the safety risks that may be generated by a product as a whole due to its digital components, including AI systems, are duly prevented and mitigated. For instance, increasingly autonomous robots, whether in the context of manufacturing or personal assistance and care should be

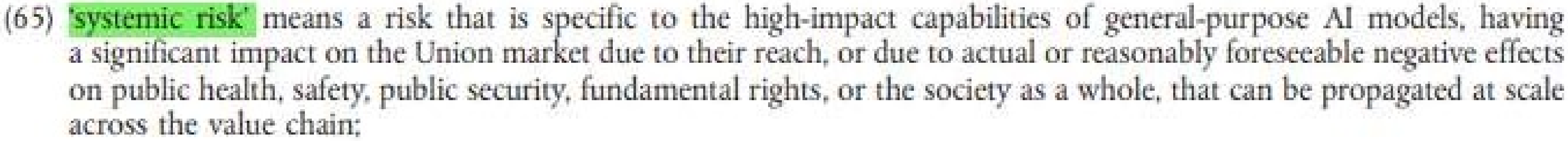


(a) the identification and analysis of the k
to health, safety or fundamental right

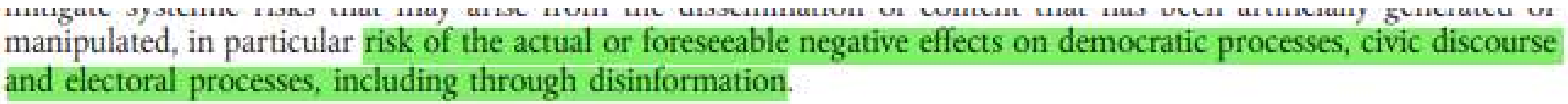
from models of making copies of themselv
can give rise to harmful bias and discrimina
disinformation or harming privacy with th



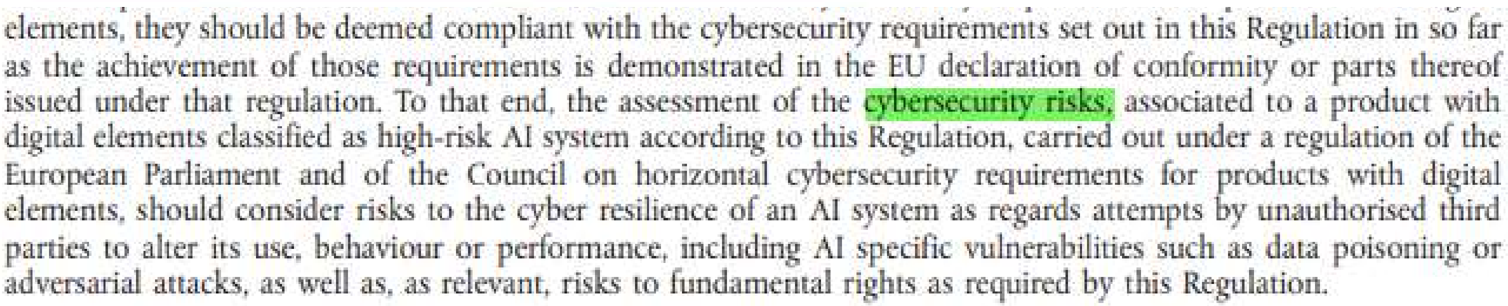
(125) Given the complexity of high-risk AI systems and the risks that are associated with them, it is important to develop an adequate conformity assessment procedure for high-risk AI systems involving notified bodies, so-called third party conformity assessment. However, given the current experience of professional pre-market certifiers in the field of product safety and the different nature of risks involved, it is appropriate to limit, at least in an initial phase of application of this Regulation, the scope of application of third-party conformity assessment for high-risk AI systems other than those related to products. Therefore, the conformity assessment of such systems should be carried out as a general rule by the provider under its own responsibility, with the only exception of AI systems



(65) 'systemic risk' means a risk that is specific to the high-impact capabilities of general-purpose AI models, having a significant impact on the Union market due to their reach, or due to actual or reasonably foreseeable negative effects on public health, safety, public security, fundamental rights, or the society as a whole, that can be propagated at scale across the value chain;

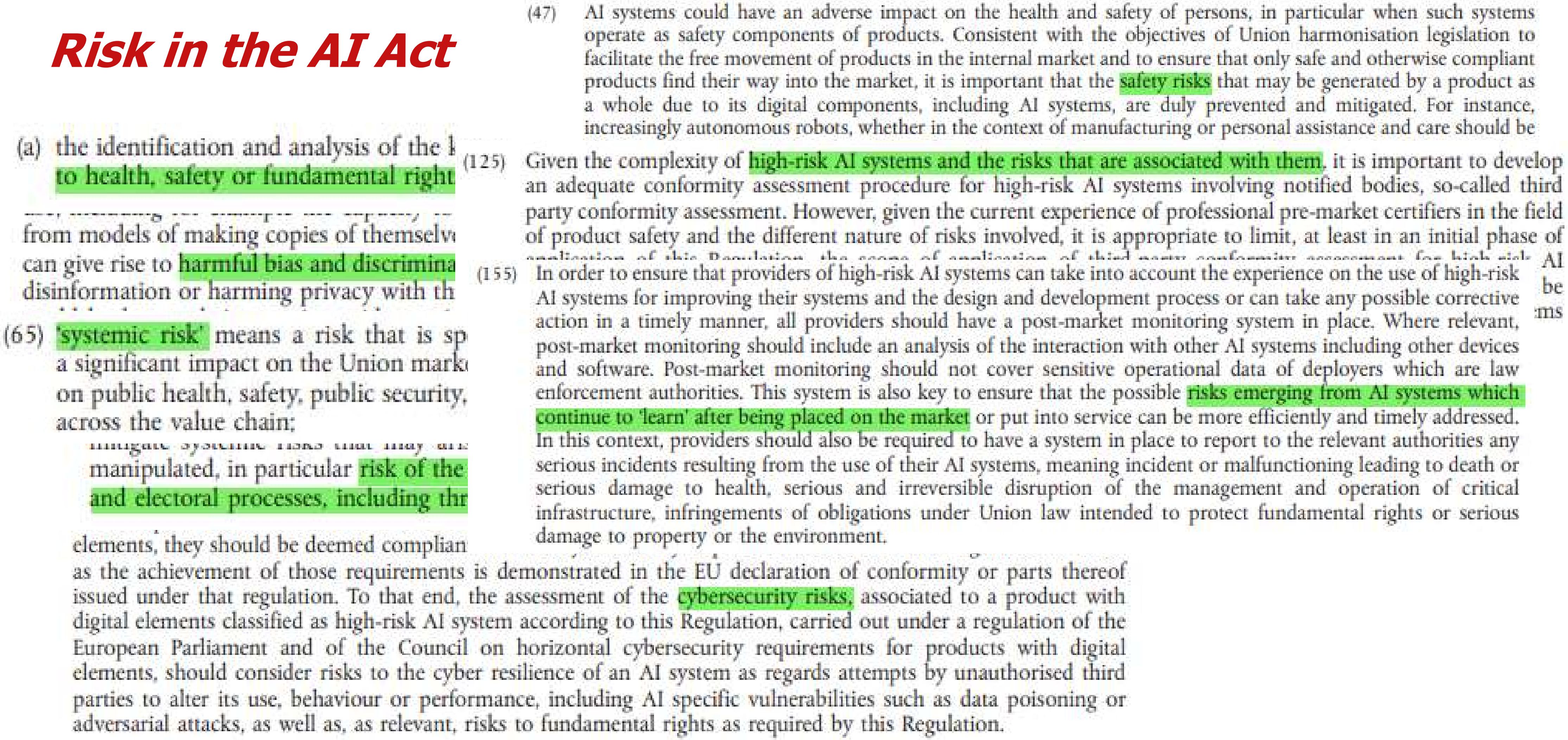


mitigate systemic risks that may arise from the dissemination of content that has been artificially generated or manipulated, in particular risk of the actual or foreseeable negative effects on democratic processes, civic discourse and electoral processes, including through disinformation.



elements, they should be deemed compliant with the cybersecurity requirements set out in this Regulation in so far as the achievement of those requirements is demonstrated in the EU declaration of conformity or parts thereof issued under that regulation. To that end, the assessment of the cybersecurity risks, associated to a product with digital elements classified as high-risk AI system according to this Regulation, carried out under a regulation of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements, should consider risks to the cyber resilience of an AI system as regards attempts by unauthorised third parties to alter its use, behaviour or performance, including AI specific vulnerabilities such as data poisoning or adversarial attacks, as well as, as relevant, risks to fundamental rights as required by this Regulation.

Risk in the AI Act



(47) AI systems could have an adverse impact on the health and safety of persons, in particular when such systems operate as safety components of products. Consistent with the objectives of Union harmonisation legislation to facilitate the free movement of products in the internal market and to ensure that only safe and otherwise compliant products find their way into the market, it is important that the safety risks that may be generated by a product as a whole due to its digital components, including AI systems, are duly prevented and mitigated. For instance, increasingly autonomous robots, whether in the context of manufacturing or personal assistance and care should be

(125) Given the complexity of high-risk AI systems and the risks that are associated with them, it is important to develop an adequate conformity assessment procedure for high-risk AI systems involving notified bodies, so-called third party conformity assessment. However, given the current experience of professional pre-market certifiers in the field of product safety and the different nature of risks involved, it is appropriate to limit, at least in an initial phase of application of this Regulation, the scope of application of third party conformity assessment for high-risk AI

be

ms

(155) In order to ensure that providers of high-risk AI systems can take into account the experience on the use of high-risk AI systems for improving their systems and the design and development process or can take any possible corrective action in a timely manner, all providers should have a post-market monitoring system in place. Where relevant, post-market monitoring should include an analysis of the interaction with other AI systems including other devices and software. Post-market monitoring should not cover sensitive operational data of deployers which are law enforcement authorities. This system is also key to ensure that the possible risks emerging from AI systems which continue to 'learn' after being placed on the market or put into service can be more efficiently and timely addressed. In this context, providers should also be required to have a system in place to report to the relevant authorities any serious incidents resulting from the use of their AI systems, meaning incident or malfunctioning leading to death or serious damage to health, serious and irreversible disruption of the management and operation of critical infrastructure, infringements of obligations under Union law intended to protect fundamental rights or serious damage to property or the environment.

(a) the identification and analysis of the k
to health, safety or fundamental right

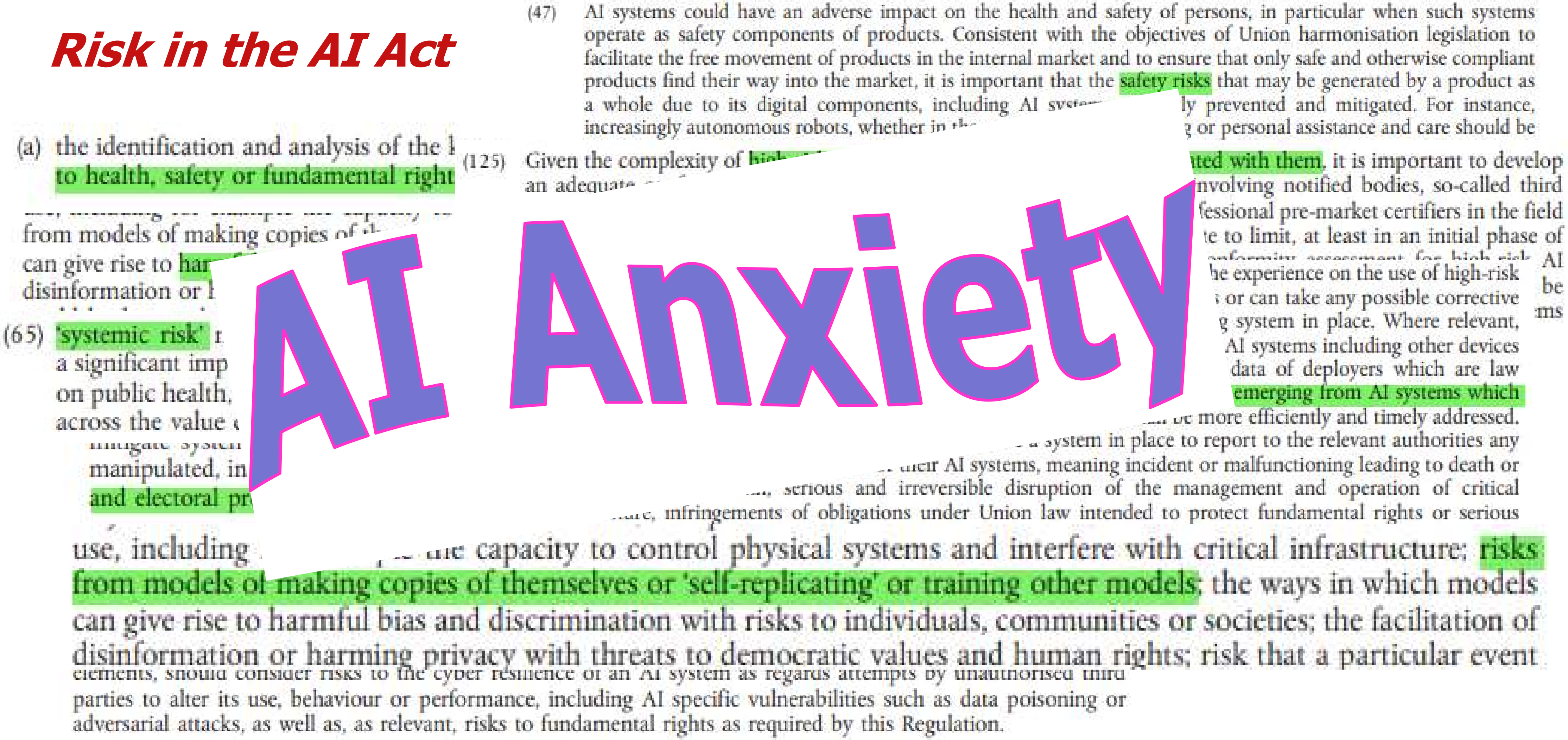
from models of making copies of themselv
can give rise to harmful bias and discrimina
disinformation or harming privacy with th

(65) 'systemic risk' means a risk that is sp
a significant impact on the Union mark
on public health, safety, public security,
across the value chain;

mitigate systemic risks that may aris
manipulated, in particular risk of the
and electoral processes, including thr

elements, they should be deemed complian
as the achievement of those requirements is demonstrated in the EU declaration of conformity or parts thereof issued under that regulation. To that end, the assessment of the cybersecurity risks, associated to a product with digital elements classified as high-risk AI system according to this Regulation, carried out under a regulation of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements, should consider risks to the cyber resilience of an AI system as regards attempts by unauthorised third parties to alter its use, behaviour or performance, including AI specific vulnerabilities such as data poisoning or adversarial attacks, as well as, as relevant, risks to fundamental rights as required by this Regulation.

Risk in the AI Act



(47) AI systems could have an adverse impact on the health and safety of persons, in particular when such systems operate as safety components of products. Consistent with the objectives of Union harmonisation legislation to facilitate the free movement of products in the internal market and to ensure that only safe and otherwise compliant products find their way into the market, it is important that the safety risks that may be generated by a product as a whole due to its digital components, including AI syst
ly prevented and mitigated. For instance, increasingly autonomous robots, whether in th
or personal assistance and care should be

(a) the identification and analysis of the k
to health, safety or fundamental right

(125) Given the complexity of hi
ted with them, it is important to develop an adequate
involving notified bodies, so-called third
fessional pre-market certifiers in the field
te to limit, at least in an initial phase of
conformity assessment for high-risk AI
be
ms
he experience on the use of high-risk
or can take any possible corrective
g system in place. Where relevant,
AI systems including other devices
data of deployers which are law
emerging from AI systems which
be more efficiently and timely addressed.
a system in place to report to the relevant authorities any
their AI systems, meaning incident or malfunctioning leading to death or
serious and irreversible disruption of the management and operation of critical
ture, infringements of obligations under Union law intended to protect fundamental rights or serious

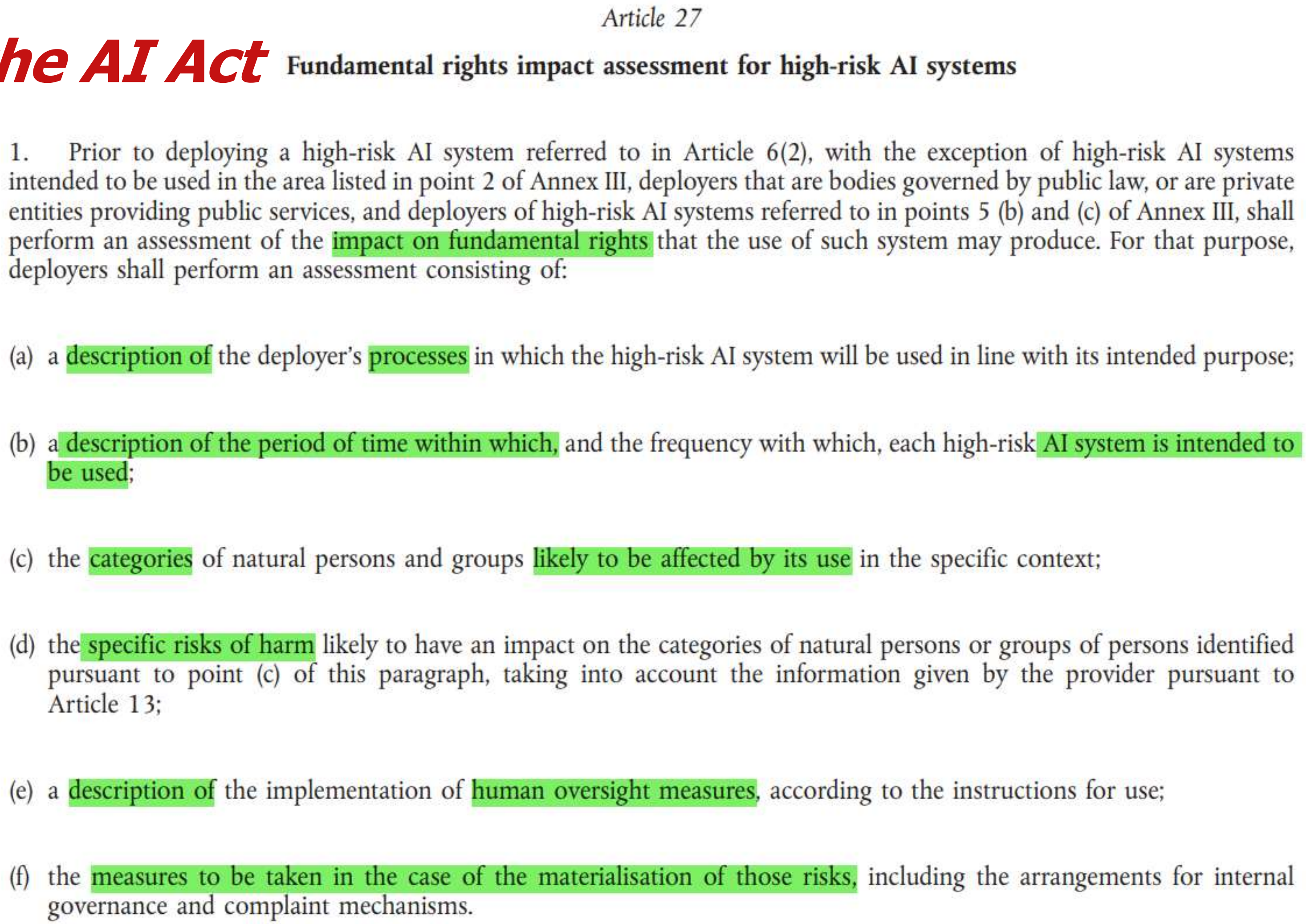
from models of making copies of th
can give rise to har
disinformation or h

(65) 'systemic risk' r
a significant imp
on public health,
across the value c
mitigate system
manipulated, in
and electoral pr

use, including
the capacity to control physical systems and interfere with critical infrastructure; risks from models of making copies of themselves or 'self-replicating' or training other models; the ways in which models can give rise to harmful bias and discrimination with risks to individuals, communities or societies; the facilitation of disinformation or harming privacy with threats to democratic values and human rights; risk that a particular event

elements, should consider risks to the cyber resilience of an AI system as regards attempts by unauthorised third parties to alter its use, behaviour or performance, including AI specific vulnerabilities such as data poisoning or adversarial attacks, as well as, as relevant, risks to fundamental rights as required by this Regulation.

Risk Assessment in the AI Act



Article 27

Fundamental rights impact assessment for high-risk AI systems

1. Prior to deploying a high-risk AI system referred to in Article 6(2), with the exception of high-risk AI systems intended to be used in the area listed in point 2 of Annex III, deployers that are bodies governed by public law, or are private entities providing public services, and deployers of high-risk AI systems referred to in points 5 (b) and (c) of Annex III, shall perform an assessment of the impact on fundamental rights that the use of such system may produce. For that purpose, deployers shall perform an assessment consisting of:

(a) a description of the deployer's processes in which the high-risk AI system will be used in line with its intended purpose;

(b) a description of the period of time within which, and the frequency with which, each high-risk AI system is intended to be used;

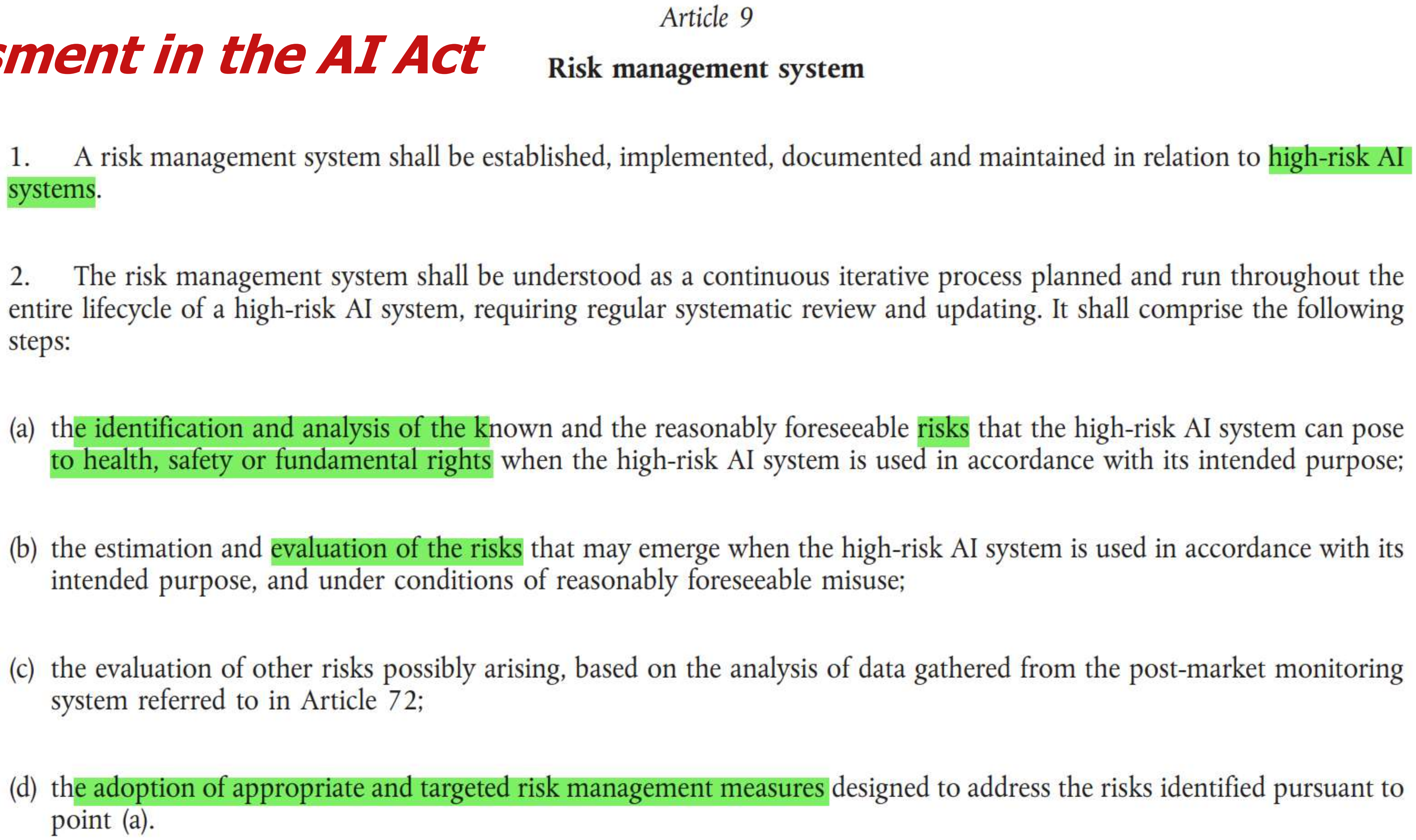
(c) the categories of natural persons and groups likely to be affected by its use in the specific context;

(d) the specific risks of harm likely to have an impact on the categories of natural persons or groups of persons identified pursuant to point (c) of this paragraph, taking into account the information given by the provider pursuant to Article 13;

(e) a description of the implementation of human oversight measures, according to the instructions for use;

(f) the measures to be taken in the case of the materialisation of those risks, including the arrangements for internal governance and complaint mechanisms.

Risk Assessment in the AI Act



Article 9

Risk management system

1. A risk management system shall be established, implemented, documented and maintained in relation to high-risk AI systems.

2. The risk management system shall be understood as a continuous iterative process planned and run throughout the entire lifecycle of a high-risk AI system, requiring regular systematic review and updating. It shall comprise the following steps:

(a) the identification and analysis of the known and the reasonably foreseeable risks that the high-risk AI system can pose to health, safety or fundamental rights when the high-risk AI system is used in accordance with its intended purpose;

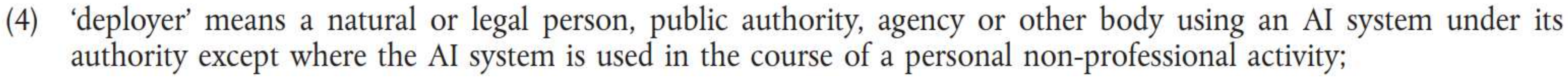
(b) the estimation and evaluation of the risks that may emerge when the high-risk AI system is used in accordance with its intended purpose, and under conditions of reasonably foreseeable misuse;

(c) the evaluation of other risks possibly arising, based on the analysis of data gathered from the post-market monitoring system referred to in Article 72;

(d) the adoption of appropriate and targeted risk management measures designed to address the risks identified pursuant to point (a).

Risk Assessment in the AI Act

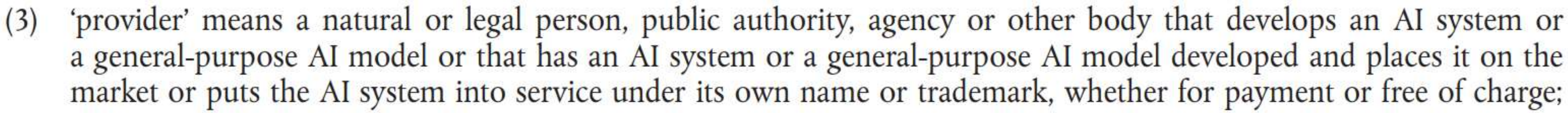
- FRIA (Art. 27 AIA):



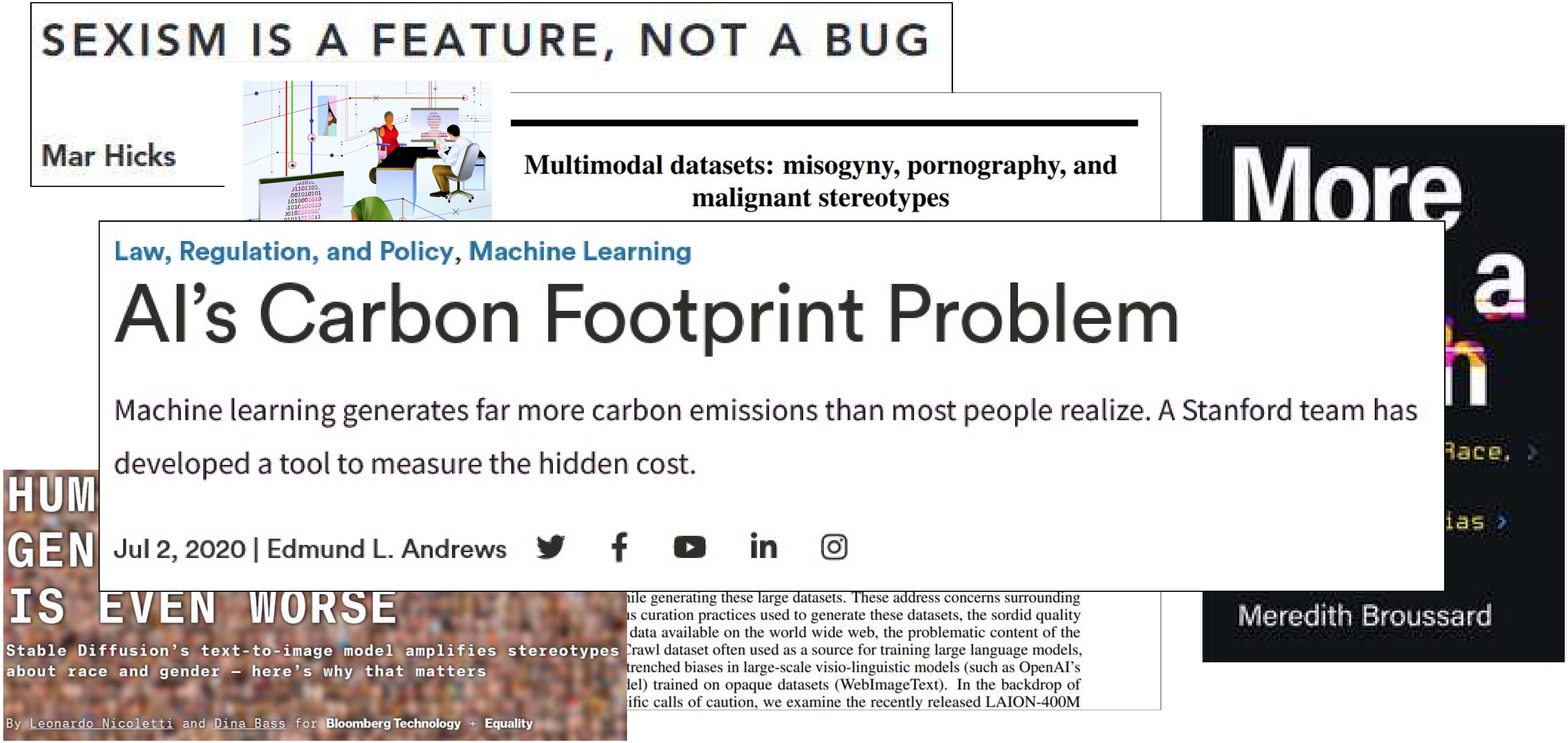
(4) ‘deployer’ means a natural or legal person, public authority, agency or other body using an AI system under its authority except where the AI system is used in the course of a personal non-professional activity;

  - But only if governed by public law, private entity providing essential services or AI systems for credit scoring or life and health insurance

- Risk Management System (Art. 9 AIA):



(3) ‘provider’ means a natural or legal person, public authority, agency or other body that develops an AI system or a general-purpose AI model or that has an AI system or a general-purpose AI model developed and places it on the market or puts the AI system into service under its own name or trademark, whether for payment or free of charge;



SEXISM IS A FEATURE, NOT A BUG

Mar Hicks

Multimodal datasets: misogyny, pornography, and malignant stereotypes

ile generating these large datasets. These address concerns surrounding
s curation practices used to generate these datasets, the sordid quality
data available on the world wide web, the problematic content of the
rawl dataset often used as a source for training large language models,
trenched biases in large-scale visio-linguistic models (such as OpenAI's
lel) trained on opaque datasets (WebImageText). In the backdrop of
ific calls of caution, we examine the recently released LAION-400M

More
a
h
Race,
ias
Meredith Broussard

Law, Regulation, and Policy, Machine Learning

AI's Carbon Footprint Problem

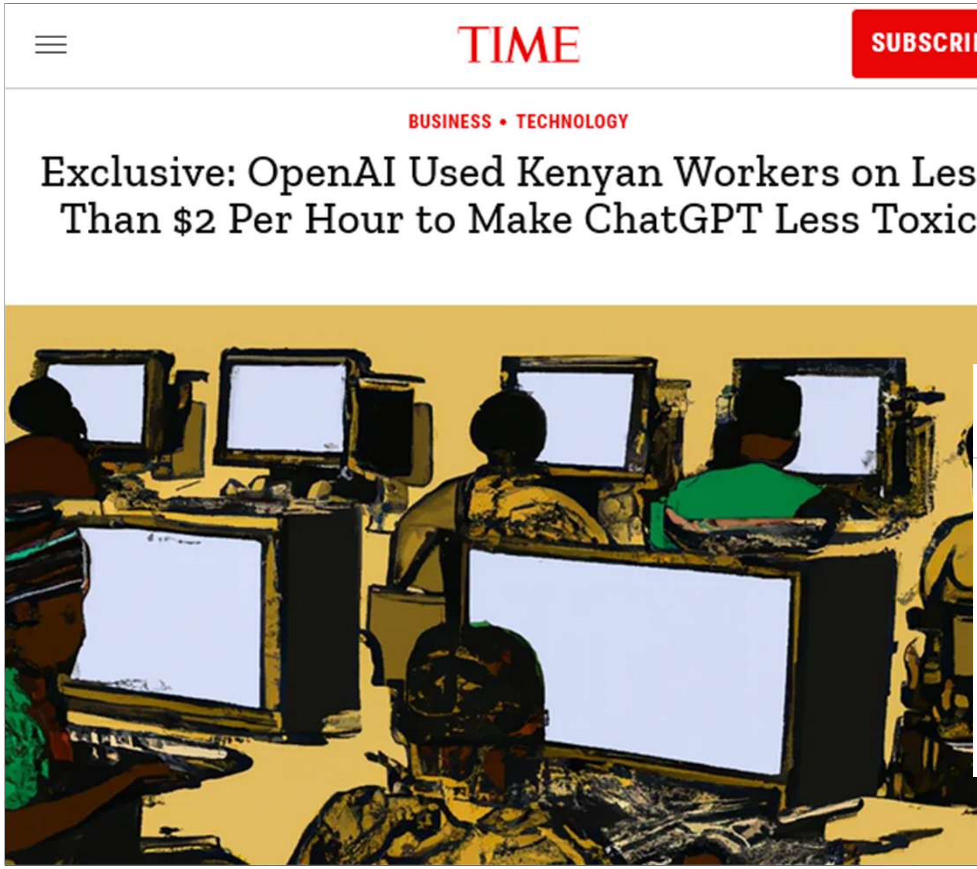
Machine learning generates far more carbon emissions than most people realize. A Stanford team has developed a tool to measure the hidden cost.

Jul 2, 2020 | Edmund L. Andrews

HUM
GEN
IS EVEN WORSE

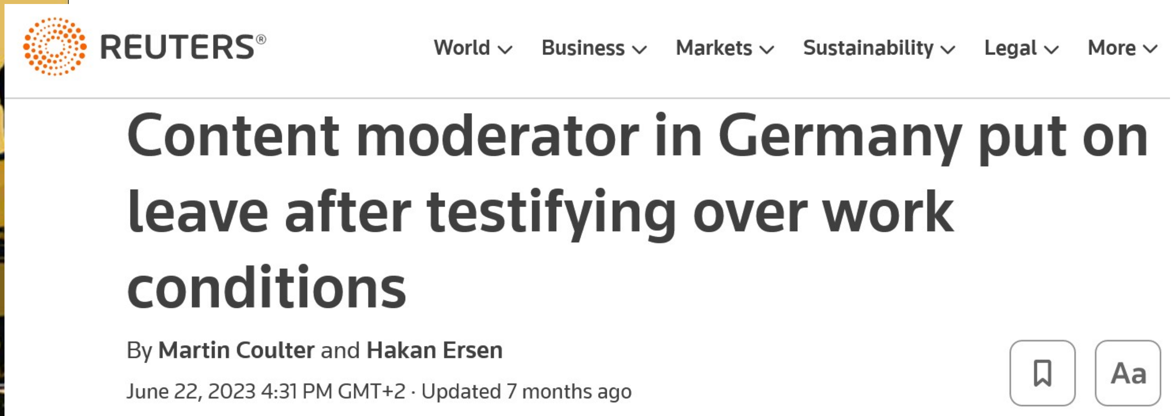
Stable Diffusion's text-to-image model amplifies stereotypes about race and gender — here's why that matters

By Leonardo Nicoletti and Dina Bass for Bloomberg Technology + Equality



BUSINESS • TECHNOLOGY

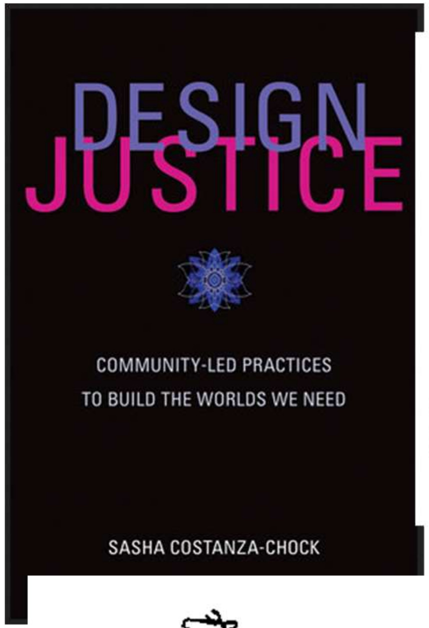
Exclusive: OpenAI Used Kenyan Workers on Less Than $2 Per Hour to Make ChatGPT Less Toxic



Content moderator in Germany put on leave after testifying over work conditions

By **Martin Coulter** and **Hakan Ersen**

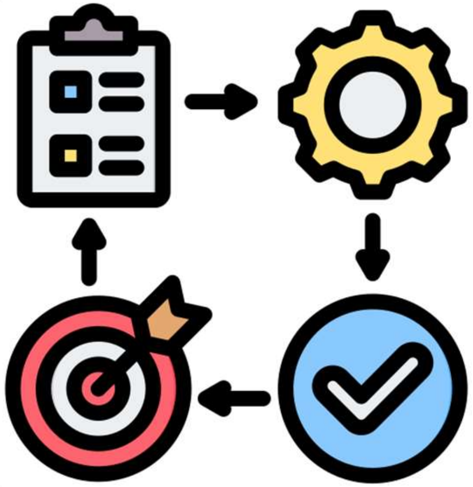
June 22, 2023 4:31 PM GMT+2 · Updated 7 months ago



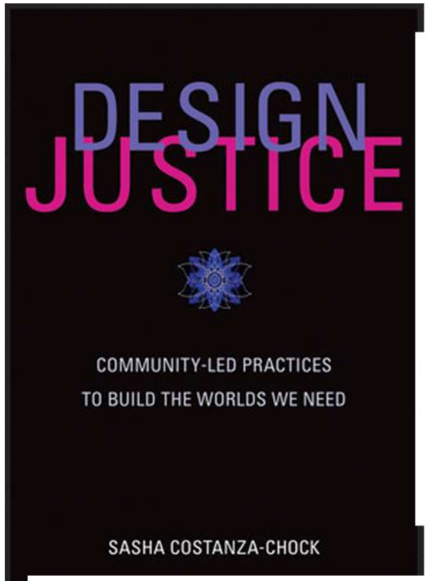
DESIGN JUSTICE

COMMUNITY-LED PRACTICES TO BUILD THE WORLDS WE NEED

SASHA COSTANZA-CHOCK



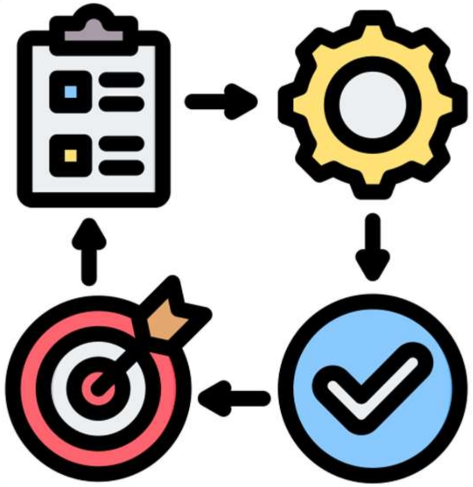
Cover illustration for "Nothing About Us Without Us: Developing Innovative Technologies For, By and With Disabled Persons" by David Werner, 1998, http://www.dinf.ne.jp/doc/english/global/david/dwe001/dwe00101.html



DESIGN JUSTICE

COMMUNITY-LED PRACTICES TO BUILD THE WORLDS WE NEED

SASHA COSTANZA-CHOCK



NOTHING ABOUT US
WITHOUT US

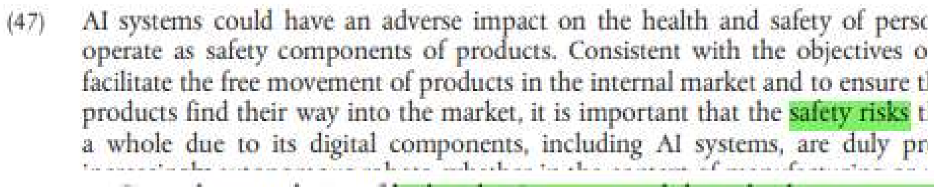
Cover illustration for "Nothing About Us Without Us: Developing Innovative Technologies For, By and With Disabled Persons" by David Werner, 1998, http://www.dinf.ne.jp/doc/english/global/david/dwe001/dwe00101.html

VS

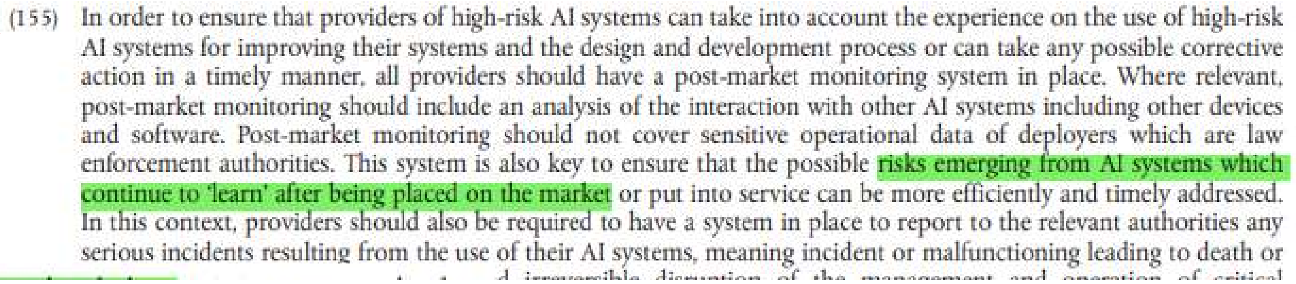
nextvoyage via Pixabay

https://www.flaticon.com/free-icons/revenue" title="Revenue icons"

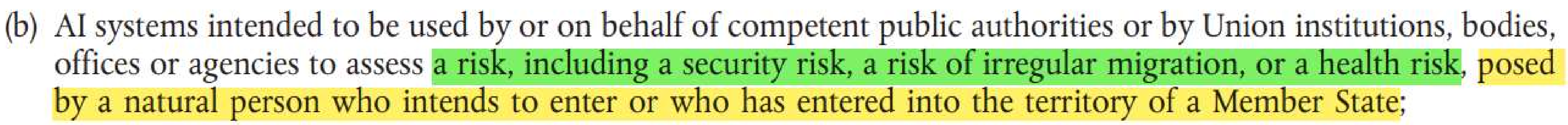
The Epitome of AI Anxiety



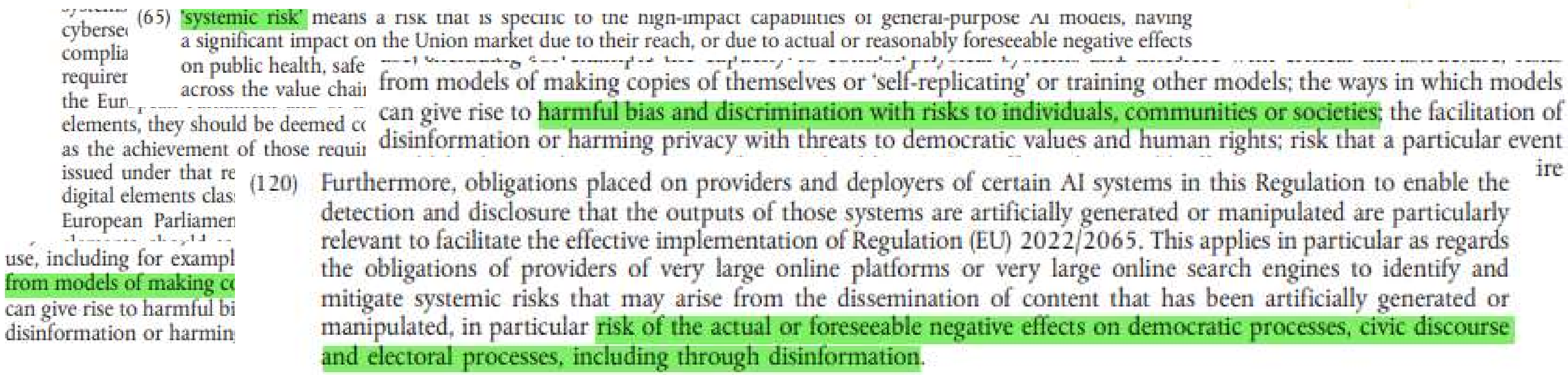
(47) AI systems could have an adverse impact on the health and safety of perso
operate as safety components of products. Consistent with the objectives o
facilitate the free movement of products in the internal market and to ensure t
products find their way into the market, it is important that the safety risks t
a whole due to its digital components, including AI systems, are duly pr



(155) In order to ensure that providers of high-risk AI systems can take into account the experience on the use of high-risk AI systems for improving their systems and the design and development process or can take any possible corrective action in a timely manner, all providers should have a post-market monitoring system in place. Where relevant, post-market monitoring should include an analysis of the interaction with other AI systems including other devices and software. Post-market monitoring should not cover sensitive operational data of deployers which are law enforcement authorities. This system is also key to ensure that the possible risks emerging from AI systems which continue to 'learn' after being placed on the market or put into service can be more efficiently and timely addressed. In this context, providers should also be required to have a system in place to report to the relevant authorities any serious incidents resulting from the use of their AI systems, meaning incident or malfunctioning leading to death or



(b) AI systems intended to be used by or on behalf of competent public authorities or by Union institutions, bodies, offices or agencies to assess a risk, including a security risk, a risk of irregular migration, or a health risk, posed by a natural person who intends to enter or who has entered into the territory of a Member State;



cyberse
complia
requirer
the Eur
elements, they should be deemed co
as the achievement of those requi
issued under that re
digital elements clas
European Parliamen

use, including for exampl
from models of making co
can give rise to harmful bi
disinformation or harmin

(65) 'systemic risk' means a risk that is specific to the high-impact capabilities of general-purpose AI models, having a significant impact on the Union market due to their reach, or due to actual or reasonably foreseeable negative effects
on public health, safe
across the value chai

from models of making copies of themselves or 'self-replicating' or training other models; the ways in which models can give rise to harmful bias and discrimination with risks to individuals, communities or societies; the facilitation of disinformation or harming privacy with threats to democratic values and human rights; risk that a particular event

ire

(120) Furthermore, obligations placed on providers and deployers of certain AI systems in this Regulation to enable the detection and disclosure that the outputs of those systems are artificially generated or manipulated are particularly relevant to facilitate the effective implementation of Regulation (EU) 2022/2065. This applies in particular as regards the obligations of providers of very large online platforms or very large online search engines to identify and mitigate systemic risks that may arise from the dissemination of content that has been artificially generated or manipulated, in particular risk of the actual or foreseeable negative effects on democratic processes, civic discourse and electoral processes, including through disinformation.

Thank you for your attention!

Dr. Felix Bieker

Office of the Data Protection
Commissioner of Schleswig-Holstein

ULD63@datenschutzzentrum.de

Plattform
Privatheit