yourself!

Question what you get. Media education to fight Disinformation

QYOURSELF GLOSSARY

Document produced by the QYOURSELF Partnership

Co-funded by
the European Union

QYOURSELF GLOSSARY

A

Algorithm: This definition is applied to the field of social media, indicating a mathematical set of rules and instructions that systematically sorts, filters, and recommends platform content for users based on how likely they are to like and interact with it.

AI (Artificial Intelligence): The theory and development of computer systems able to mimic problem-solving and decisionmaking capabilities of the human mind

Attribution: Clear identification of the actors behind a certain piece of disinformation or information campaign, which requires extreme caution.

Automation: The process of designing a machine to complete a task with little or no human direction; used – among other things – to manufacture the amplification of disinformation.

B

Bot: A software program that performs automated, repetitive, pre-defined tasks, typically imitating or replacing human behaviour.

C

Chatbot: A computer program that can chat with its users. Chatbots simulate conversations by sending automatic or predefined messages, synthesising voice, or offering decision buttons.

Cheapfake: The term was coined by Britt Paris and Joan Donovan to indicate altered media that has been manipulated without advanced processing technologies (differently from deepfakes), e.g., by speeding or slowing footage.

Clickbait: The practice of writing sensationalised, misleading, or false headlines in order to attract clicks on a piece of content and therefore encourage traffic.

Climate delayism: A systematic and coordinated strategy to baselessly question climate actions to slow down or postpone indefinitely those actions.

Climate doomism: The convictions that the battle against climate change is already lost and, therefore, climate actions or policies are pointless.

Code of Practice on Disinformation: A tool (launched in 2018 and updated in 2022) that brings together major tech platforms, players in the advertising industry, fact-checkers, research and civil society organisations (signatories to the Code) in the fight against disinformation through a set of voluntary commitments and measures. The signatories to the Code decide which commitments they sign up to. It is their responsibility to ensure the implementation of these commitments.

Confirmation bias: The tendency to interpret information in a way that confirms what one already believes. For instance, during an election, people tend to believe information that paints the candidate they support positively, while dismissing information that portrays them negatively.

Conspiracy theory: The belief that a small group of powerful people are making secret arrangements to advance their personal interests, consequently causing harm to society.

Content moderation: The organised practice of screening user-generated content online to determine the appropriateness of the content for a given site, locality, or jurisdiction. Actions range from reducing content visibility to content and user suppression. Content moderation techniques include manual pre-moderation, manual post-moderation, reactive moderation, distributed moderation, or automated moderation.

Cookie: Information stored on an Internet user's computer for session management (e.g., recall their individual login information and preferences), personalisation (e.g., using the recorded information for targeted ads), and tracking purposes (e.g., keeping items in online shopping carts and suggesting similar products).

D

Dangerous speech: Dangerous speech is any form of expression (e.g., speech, text, or images) that can increase the risk that its audience will condone or commit violence against members of another group. Online disinformation and hate speech constitute dangerous speech when they include elements that can lead to offline discrimination and brutality.

Data anonymisation: The process of protecting private or sensitive information by erasing or hashing identifiers that connect an individual to stored data, so that the data is retained but the source remains anonymous.

Data mining: The process of analysing big volumes of data by combining tools from statistics and artificial intelligence to recognise useful patterns. For instance, data mining techniques enable companies to predict future trends and make more informed business decisions.

Deepfake: An image or footage that has been convincingly altered and manipulated through some form of machine learning (differently from cheapfakes) to misrepresent someone as doing or saying something that was not actually done or said.

Deep learning: Deep learning is a subset of machine learning, which is essentially a neural network (i.e., a model made up of information interconnections) with three or more layers. These neural networks attempt to simulate the behaviour of the human brain, allowing it to learn from large amounts of data, that is to say adapting and modifying its structure based both on external data and internal information. Learning can be supervised, semi-supervised or unsupervised.

Disinformation: Information that is false and is disseminated intentionally to cause harm.

Disinformation entrepreneurs: Actors who exploit major events, such as the war in Ukraine, to spread false content or propaganda for ideological, reputational, or financial gains. Our study shows how dormant and new YouTube channels exploited the war in Ukraine to spread pro-Russian disinformation.

Disinformation-for-hire: A growing industry in which private marketing, communications, and public relations firms are paid to sow discord by spreading false information and manipulating content online. A recent Forbidden Stories piece recounts how “digital influence mercenaries” were paid to spread online gender-based disinformation against a journalist.

Doxing: The act of publishing private or identifying information about a person or organisation online, with malicious intent.

DSA (Digital Services Act): A ground-breaking legislation on Internet safety and platform accountability that regulates digital services (from simple websites to Internet infrastructure services and online platforms) operating in the European Union market or delivering services to European Union users and is a part of the Digital Services Package. The DSA entered into force in late 2022 and will become applicable to all services in early 2024. It will apply to VLOPs and VLOSEs (see definitions) earlier, several months after their designation. The DSA will create a stronger incentive structure for companies to tackle

disinformation, thanks to the harmonisation of regulatory oversight and the introduction of due diligence obligations for online platforms

E

Echo chamber: A closed ecosystem in which participants only encounter beliefs that amplify or reinforce their pre-existing beliefs on various topics. Echo chambers are a direct consequence of filter bubbles.

Encrypted messaging: Encryption converts human-readable plaintext into so-called ciphertext (i.e., encrypted text transformed from plaintext using an encryption algorithm) to ensure secrecy. For example, end-to-end encryption ensures only the sender and the receiver can read or listen to what is sent.

EMFA (European Media Freedom Act): A proposal for a regulation to strengthen media freedom and plurality in Europe. It deals with media ownership transparency, funding for public service media, spyware against journalists and media content online, among other issues. The latter is a concerning matter for the counter-disinformation community as it has opened the door for the media exemption (see definition) to come back in the legislative process. If adopted, it would create a massive loophole for disinformation and undo any progress that has been achieved in countering disinformation in the last years.

F

Fabricated content: Content that is 100% false, designed to deceive and do harm. To illustrate this, Hitler never said that Black people are the “true Hebrews” as some claimed on social media. This is part of First Draft’s typology to classify mis- and disinformation.

Fact-checking: The process of verifying information to promote the veracity and correctness of reporting and statements. Counting on over a hundred verified signatories; the International Fact-checking Network (IFCN) created a Code of Practice for fact-checking organisations.

Factoid: A piece of information or news that is repeated so often that it is believed to be true. An example is the belief that the Great Wall of China is visible from the moon.

Fake news: False or misleading information presented as news. Although it can be inaccurately used as a synonym of disinformation, the term has been popularised by Donald Trump, who exploited it to cast doubt upon credible news.

False connection: When the content is not supported by headlines, visuals, or captions. In early 2022, photos from Gaza were reshared online with captions claiming to show explosions in Ukraine. This is part of First Draft's typology to classify mis- and disinformation.

False context: Genuine content that is shared with false contextual information. For instance, the authentic news that a nurse had fainted after receiving the COVID-19 vaccine in late 2020 was shared online with false contextual information that it was due to the lethality of the vaccine, rather than a vagal reaction. This is part of First Draft's typology to classify mis- and disinformation.

Filter bubble: A state of intellectual isolation that can result from personalised searches when a website algorithm selects what information a user would like to see based on information about the user, enabling a self-confirming feed exclusively based on content that fits the user's preferences.

FIMI (Foreign Information and Manipulation Interference): The European External Action Service (EEAS) defines it as "a mostly non-illegal pattern of behaviour that threatens or has the potential to negatively impact values, procedures and political processes. Such activity is manipulative in character, conducted in an intentional and coordinated manner. Actors of such activity can be state or non-state actors, including their proxies inside and outside of their own territory".

Firehosing: A propaganda technique by which many messages are broadcast rapidly, repetitively, and continuously over multiple online channels without considering truthfulness or consistency.

Freedom of speech: The power or right to express one's opinions without censorship, restraint, or legal penalty. It is often weaponised to reject content moderation, although disinformation limits the targeted group's possibility to practice their freedom of speech

G

Gaslighting: A form of psychological manipulation in which the abuser attempts to sow self-doubt and confusion in their victim's mind

GDPR (General Data Protection Regulation): A regulation in European law on data protection and privacy in the European Union and the European Economic Area. Its primary aim is to enhance individuals' control and rights over their personal data and to simplify the regulatory environment for international business.

Gender-based disinformation: The spread of deceptive or inaccurate information and images against women – especially in positions of power and visibility. It frames them as untrustworthy, unintelligent, emotional, or sexual to alter the public's understanding of their track records. The intent is immediate political gain, as well as discouraging women looking into political careers or leadership roles.

Gender ideology or gender theory: Simply concerned with understanding and accepting cross-cultural similarities and differences in human views on women, men, and alternative gender identities, the concept was adopted by a global movement to articulate opposition to gender equality, reproductive rights, sexual education, and LGBTQ+ rights.

Great Replacement: A far-right conspiracy theory according to which white European populations are being demographically and culturally replaced with non-white peoples

(especially from Muslim countries) through mass migration, demographic growth, and a drop in the birth rate of white Europeans.

Great Reset: An economic recovery plan launched by the World Economic Forum's (WEF) after COVID-19. The term also refers to a growing online conspiracy theory that considers the WEF a global elite who is using the pandemic to seize control of the global economy and impose radical social change.

H

Hack-and-leak: A tactic that combines a cyber-attack and an information operation, also falling into the category of malinformation. The leaked contents may be authentic, fabricated, doctored or a mix of all these

Hacktivism: The act of hacking or breaking into a computer system, for politically or socially motivated purposes.

Harmful content: Content that does not always strictly fall under legal prohibitions but that might nevertheless have harmful effects, such as disinformation.

Hate speech: Discourse that expresses hate or encourages violence towards a person or group based on inherited characteristics such as race, religion, sex, or sexual orientation. On 9 December 2021, the European Commission adopted a Communication prompting a Council decision to extend the current list of 'EU crimes' in Article 83(1) TFEU to hate crimes and hate speech.

Hoax: A deception or falsehood, which we use in general terms to indicate a single piece of mis- or disinformation.

I

Illegal content: Information items that are not compliant with a given legislation, such as hate speech, terrorism, incitement to violence, child abuse material, or intellectual property breaches. Disinformation is harmful but not necessarily illegal.

Imposter content: The impersonation of genuine sources (e.g., see Doppelganger). This is part of First Draft's typology to classify mis- and disinformation.

Influence operations: Term used primarily in the context of military operations, as well as by social networks sometimes, to indicate the deliberate and coordinated attempts of unidentified actors to manipulate the public debate using inauthentic accounts and inaccurate information.

Infodemic: A rapid and far-reaching spread, online and offline, of an excessive amount of both accurate and inaccurate information about an event, such as a disease outbreak.

Information disorder: A collective term coined by Claire Wardle to refer to indicate disinformation, misinformation, and malinformation.

J

Junk site: A website – also known as "content farm" – that contains large quantities of low-quality content (and often false and hyper-partisan). It is either created or aggregated from other websites for the purpose of improving its search engine rankings.

To be classified as such, an outlet would need to fulfil three out of five criteria regarding: poor professionalism, sensationalistic style, lack of credibility, high bias, and use of counterfeit content.

K

Kalergi plan: A far-right, antisemitic conspiracy theory, which denounces an alleged plot to mix white Europeans with other races via immigration (see also Great Replacement).

Kompromat: Damaging information about a prominent or visible person, which may be used to create negative publicity, blackmail, and extortion.

L

Lawful but awful: A speech or action that cannot be prohibited by law (including the terms of service of platforms) but that profoundly violates many people's sense of decency, morality, or justice.

M

Malign actors: General term – also known as "malicious actors" – used to describe those who intentionally create or spread disinformation.

Malinformation: Information that is based on reality but is used to harm or threaten a person, an organisation, or a country (e.g., see "doxing").

Manipulated content: When genuine information or imagery is manipulated to deceive, for instance in the form of a doctored photo, video, or text. This is part of First Draft's typology to classify mis- and disinformation.

Meme: An amusing or interesting visual item (e.g., photo, screenshot, cartoon, or video) that spreads widely online. In the context of disinformation, they may be used to mislead or spread false information in a humorous or culturally-relevant way, or if the audience believes that what they are seeing is true.

Metaverse: A virtual-reality space in which users can interact with a computer-generated environment and other users.

Micro-targeting: A marketing strategy that employs users' data (i.e., collected via cookies) to segment them into groups for content targeting. It has been used for malicious purposes, especially during elections to target voters with personalised political advertisements.

MIL (Media and Information Literacy): The Moscow Declaration on Media and Information Literacy (2012) defines it as "a combination of knowledge, attitudes, skills, and practices required to access, analyse, evaluate, use, produce, and communicate information and knowledge in creative, legal and ethical ways that respect human rights". High levels of MIL contribute to society's information resilience.

Misinformation: Information that is false, but believed to be true by those disseminating it. It differs from disinformation in the absence of an intention to mislead or harm. For instance, during the pandemic, many people shared doctored images of wild animals flourishing in quarantined cities, thinking they were true.

Misleading content: Misleading use of information to frame an issue or an individual. A recurrent hoax in Italy is that “migrants receive 30 Euros per day”. This is a misleading statement drawn from a 2014 document reporting a call for bids to infrastructures hosting migrants, whose spending for the reception of asylum-seekers should not exceed 30 Euros per day per person. This is part of First Draft’s typology to classify mis- and disinformation.

N

New World Order: A conspiracy theory about a secretive power elite with a globalist agenda (i.e., the Illuminati), who is conspiring to eventually rule the world through an authoritarian one-world government

O

Online platform: A digital service that uses the Internet to facilitate interactions between two or more separate but interdependent users (whether they are companies or private individuals).

OSINT (Open-Source Intelligence): The collection and analysis of data gathered from publicly available sources to produce actionable intelligence.

P

Phishing: A fraudulent practice, which is usually part of a hacking attempt, consisting of sending messages – usually emails and direct messages – purporting to be from

reputable companies in order to induce individuals to reveal personal details, such as financial information.

PII (Personally Identifiable Information): Information that, when used alone or combined with other relevant data, can identify an individual (including direct identifiers and passport information and quasi-identifiers are race).

Post-truth: A situation in which emotions and beliefs shape public opinion; rather than facts

Propaganda: True or false information spread to persuade an audience, which is often politically connoted. In detail, white propaganda uses accurate, albeit selectively presented, information and identified sources.

Pwned: A term that originated in video game culture and means “owned”, in the sense that someone’s personal data has been violated and its confidentiality compromised.

Q

Questionable-cause logical fallacy: The fallacious idea that “correlation implies causation” and thus, two events occurring simultaneously are assumed to have a cause-and-effect relationship. This fallacy is at the basis of conspiracy thinking.

R

Radicalisation: A phased and complex process by which an individual or a group embraces a radical ideology or belief that accepts, uses, or condones violence, including acts of terrorism, to reach a specific political or ideological purpose.

Report: On social media, it is the process through which users can ask for content in violation of the platform's policies to be removed or its access restricted.

S

Scam: A fraudulent or deceptive act or operation, usually via email or private message.

Scraping: Web scraping, web harvesting, or web data extraction is the process of extracting data from a website. Such programs are made to emulate human browsing on the web. While web scraping can be done manually by a user, the term generally refers to automated processes implemented using a specifically crafted web crawler.

Sock puppet: A fictitious online identity created specifically to deceive, i.e., a fake persona. Sock puppet accounts differ from catfishing as the former are short-lasting, not very detailed, and not necessarily conceived for malign intent.

Spam: Unsolicited or irrelevant online messages, typically sent to a large number of users for the purpose of promoting, advertising, or scamming an audience.

Synthetic media: Also known as “AI-generated media”. It is a catch-all term for the artificial production, manipulation, and modification of data and media by automated means, especially using artificial intelligence algorithms, such as for the purpose of misleading people or changing an original meaning (e.g., deepfakes).

T

Technological optimism: The belief that problems such as pollution, resource depletion, and overpopulation can be solved entirely through the proper applications of advanced technology. The position is often adopted in conjunction with climate change denialism and delayism.

ToS (Terms of Service): A document stating details about what a service provider is responsible for as well as user obligations that must be adhered to for continuation of the service.

Troll: A user who intentionally antagonises others online by posting inflammatory, insulting, or disruptive content to get attention, upset, or provoke.

TTPs (Tactics, Techniques, and Procedures): This is the term used by cyber-security professionals to describe the behaviours, processes, actions, and strategies used by a malign actor to develop threats and engage in cyber-attacks. Tactics are the high-level description of an actor’s behaviour. Techniques are a more detailed, medium-level, description of a behaviour in the context of a tactic. Procedures are the low-level, highly detailed description in the context of a technique.

U

-

V

Virality: The tendency of an image, video, or piece of information to be circulated rapidly and widely from one Internet user to another, regardless of its authenticity.

Vishing: A combination of 'voice' and 'phishing', it indicates a phone scam that uses social engineering tactics to persuade victims to provide personal information, typically with the goal of accessing financial accounts. Users are often tricked into believing that their bank account was compromised or that they received an unmissable offer.

VPN (Virtual Private Network): A non-physical network to which access is provided upon authentication and authorisation. It is used to encrypt the user's network traffic in a way that does not expose information regarding their IP address and geolocation.

W

-washing: A deceitful marketing strategy that consists in pretending to defend a socially desirable cause to improve one's reputation rather than actually backing it up with genuine action. Examples include greenwashing (when an organisation provides the appearance of being environmentally conscious without any substance); wokewashing (appearing to promote social justice), purpose-washing (appearing to promote a cause-based purpose), or genderwashing (appearing to promote gender equality).

Web tracker: A piece of code that gets executed by the browser each time a user visits the webpage that contains it. Web trackers gather data on how users interact with the websites, the number of visits and times spent on the page, the scrolling speed and other

relevant information that allow web administrators to know more about their public and thus target specific audiences.

Website defacement: A form of cyber-attack on a website or web page that changes its visual appearance, modifying or replacing the hosted content

X

-

Y

-

Z

Zoom bombing: The unwanted and disruptive intrusion of Internet trolls into a video-conference call, generally displaying offensive behaviour and obscene material. Zoom fixed the issue by enhancing security features (i.e., enabling a waiting room, providing passwords, allowing the host to approve or block user entries), but the unpleasant phenomenon might still occur.

yourself

Question what you get. Media education to fight Disinformation

Universidad del País Vasco UPV/EHU - University of the Basque Country UPV/EHU
Spain
www.ehu.eus

IBERIKA EDUCATION GROUP GGMBH
Germany
www.iberika.de

STIMMULI FOR SOCIAL CHANGE
Greece
stimmuli.eu

CESIE ETS
Italy
cesie.org

X Liceum Ogolnoksztalcace im. prof. Stefana Banacha w Toruniu
Poland
www.xlo.torun.pl

FUNDACIÓN MALDITA.ES CONTRA LA DESINFORMACION PERIODISMO EDUCACION INVESTIGACION Y DATOS EN NUEVOS FORMATOS
Spain
maldita.es

Co-funded by the European Union

Erasmus+: Key Action 2, Cooperation partnerships in adult education
Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

Project Number: 2023-1-ES01-KA220-ADU-000153626