



# The Top Ten Fundamental Terms for Journalists Covering Internet Rights

Presented by the [African Internet Rights Alliance \(AIRA\)](#)

- 1. Network disruptions (shutdowns, blackouts, kill switches):** This refers to the disruption of electronic communications over a network rendering them inaccessible or effectively unusable for a specific population or within a particular location.<sup>1</sup> Network disruptions could be either intentional or unintentional and/or affecting partial or the totality of services, rendering them inaccessible or effectively unusable often to exert control over the flow of information.<sup>2</sup> This happens when an actor – usually a government – intentionally disrupts the Internet or mobile applications (such as WhatsApp or Telegram) to control what people say online.<sup>3 4</sup>
- 2. Surveillance and tracking:** This phrase refers to the monitoring of digital activity and data stored or transmitted over networks such as the Internet and mobile communications. Surveillance and tracking are often carried out covertly and may be done by governments,<sup>5</sup> corporate organisations, criminal outfits or even individuals.<sup>6</sup> It may or may not be legal and may or may not require authorization from a court or other independent government agencies. When such monitoring is abused, in addition to the violation of privacy, there is a direct relationship between surveillance and tracking and the freedom of expression. While surveillance does not lead directly to censorship, the perception of surveillance can lead to self-censorship.<sup>7</sup>
- 3. Data Breaches:** This is the intentional or unintentional release of secure or private and confidential information from a system without the knowledge or authorization of the system’s owner.<sup>8</sup>
- 4. Data Protection:** Data protection (data privacy or information privacy) is the process of safeguarding data from corruption, compromise or loss.<sup>9</sup> The importance of data protection increases as the amount of data created and stored continues to grow at unprecedented rates.<sup>10</sup> When data is collected, it is critical that there be safeguards in place to ensure that the use of the data is in line with human rights standards. Guarding against the abuses that can arise when data is stored by organisations, businesses or the government requires systems and safeguards.<sup>11 12</sup>

<sup>1</sup> [Disconnected Report 2018](#). Global Network Initiative.

<sup>2</sup> [Étude de cas: Cameroun: 93 jours d’arrêt d’Internet](#). Paradigm Initiative (PIN).

<sup>3</sup> [Despots and Disruptions: Five Dimensions of Internet Shutdowns in Africa](#). CIPESA.

<sup>4</sup> [Building trust between the state and citizens: A Policy Brief on Internet shutdowns and elections in Kenya 2017](#). KICTAnet.

<sup>5</sup> [Digital Rights in Africa Report 2019](#). Paradigm Initiative (PIN).

<sup>6</sup> [Africa in the Crosshairs of New Disinformation and Surveillance Schemes That Undermine Democracy](#). CIPESA.

<sup>7</sup> [Trends in transition from classical censorship to Internet censorship: selected country overviews](#). IFLA.

<sup>8</sup> [Definition of “data breach”](#). TechTarget.

<sup>9</sup> [ARTICLE 19 Data Protection Policy](#). ARTICLE 19.

<sup>10</sup> [The Data Protection Act as a tool for permitting innovation and consumer safety in Kenya’s digital finance market](#). CIPIT.

<sup>11</sup> [Policy Brief: Tanzania’s EPOCA and Cybercrimes Laws Offer No Protection for Citizen’s Data](#). Paradigm Initiative (PIN).

<sup>12</sup> [Data protection in Kenya: Policy Brief examining the current state of data protection in Kenya](#). KICTAnet.

5. **Intermediary Liability:** An intermediary is an Internet-based service provider, which provides its users with a platform to upload and share all and any types of content, ranging from text to videos. Some of the more popular examples of intermediaries would be Facebook, YouTube, Twitter, WordPress and Blogspot.<sup>13</sup> The concept of intermediary liability itself is based on economic incentives. While individuals have the incentive to say what they want to say, and put effort into ensuring that it is appropriately disseminated, an intermediary does not have such an incentive. Thus, on one hand, the individual will go out of their way to make sure what they say is being heard, perhaps even at a risk to their person. But on the other hand, intermediaries usually do not have an incentive to promote the free speech of their subscribers and users.<sup>14 15</sup>
6. **Fake News:** Fake news is a type of yellow journalism or propaganda that consists of deliberate false or misleading information spread via traditional print and broadcast news media or online media. Fake news is written and published with the intent to mislead in order to damage an agency, entity or person, and/or gain financially or politically. Fake news creators often use sensationalist, dishonest or outright fabricated headlines to increase readership, online sharing or revenue from Internet traffic.<sup>16</sup>
7. **Digital Security:** Digital security is the protection of online identities and assets. Criminals are finding new ways to operate and steal information from digital users for their own personal gain.<sup>17</sup> Digital security is an all-encompassing term which includes the tools used to secure devices, communications and data in the online and mobile world.
8. **Cybercrime:** Also called computer crime, cybercrime is the use of a computer as an instrument to further illegal ends, such as committing fraud, trafficking in child pornography and intellectual property, identity theft or violating privacy.<sup>18</sup> Cybercrime, especially through the Internet, has grown in importance as the computer has become central to commerce, entertainment and government.
9. **Access to information online:** Information access online is the freedom or ability to identify, obtain and make use of data or information effectively. The right to information provides public access to information held by public authorities or by private authorities performing public duties. Freedom of information also involves getting access to information which a person needs in order to enjoy their human rights.<sup>19</sup> It does this in two ways: Public authorities are obliged to publish certain information about their activities; and members of the public are entitled to request information from public authorities. The right to information is critical for building trust between governments and the public.<sup>20</sup>
10. **Freedom of expression online:** This is the right to express oneself online and to access information, the opinions and expressions of others. This includes political speech, religious views, opinions and expressions that are favourably received or regarded as inoffensive, but also those that may offend, shock or disturb others.<sup>21</sup> From the onset, freedom of expression is a fundamental right that is not only enjoyed offline, but online through the Internet and via other enabling digital technologies. In exercising freedom of expression, one should have due regard to the strict limitations set out in international human rights law, as well as other mutually-reinforcing rights, such as the right to privacy. Organisations, businesses and governments must respect freedom of expression online by providing an enabling environment for free expression.<sup>22</sup> This freedom is threatened by Internet censorship, which is used to control or suppress what can be accessed, published or viewed on the Internet.<sup>23</sup>

<sup>13</sup> [Internet intermediaries: The dilemma of liability in Africa](#). APC.

<sup>14</sup> [Global Expression Report 2018/19: Intermediary Liability](#). ARTICLE 19.

<sup>15</sup> [Which Intermediaries Have Your Back?: How Kenyan Intermediaries Protect Human Rights Online](#). KICTANet.

<sup>16</sup> [“Fake News” and Internet Shutdowns in Africa – What is to be Done?](#) CIPESA.

<sup>17</sup> [Digital Security](#). CcHub.

<sup>18</sup> [Cybercrime: The World’s New Social Problem](#). CcHub.

<sup>19</sup> [Universal Access to Information in Africa: What Governments Need to Do](#). CIPESA.

<sup>20</sup> [Ensuring the Public’s Right to Know in the COVID-19 Pandemic](#). ARTICLE 19

<sup>21</sup> [The Universal Declaration of Human Rights](#). United Nations.

<sup>22</sup> [Coronavirus: ARTICLE 19 briefing on tackling misinformation](#). ARTICLE 19.

<sup>23</sup> [Digital Activism and the Right to Online Free Speech and Assembly \[Case Study\]](#). Paradigm Initiative (PIN).