The concept of human rights long predates the internet. There is an existing body of international law which sets out the core principles, in particular the Universal Declaration of Human Rights of 1948 and the United Nations International Covenant on Civil and Political Rights, as well as regional instruments such as the European Convention on Human Rights and the American Convention of Human Rights. There have also, for many years, been intense discussions both about how to protect them, and how to manage situations where balance is necessary.

Nonetheless, the major transformations that the digital revolution has brought about have both accentuated debate on some questions, and raised new ones. The focus on the importance of human rights online is of course to be welcomed as a sign that the principles that are most important to us offline are also being discussed and implemented online.

This final chapter of IFLA's Internet Governance Guide for libraries focuses on some of these.

Adapting Existing Rights to a Digital Age: Freedom of Expression

While there is a broad principle that the rights we enjoy offline should be enjoyed online also, this is not always so easy. In particular, the internet has both increased the power and reach of free expression, but also created new ways of restricting or blocking it.

Freedom of expression is the power or right to express one's opinions without censorship, restraint, or legal penalty. It is protected by global instruments such as the Universal Declaration of Human Rights (made legally binding by the International Convention on Civil and Political Rights). These texts do underline that there are limits, for example incitement to discrimination, or other situations where it could limit the rights of others, with plenty of law and practice concentrating on where the limits of free speech should lie.

Freedom of Expression has been affirmed as a key principle in the online world, notably by the UN Human Rights Council Resolution on Protection of Freedom of Expression on the Internet drafted in 2012, and regular reports by the UN Special Rapporteur. This work underlines the potential of the internet to give more people a louder voice than ever before.

Yet as highlighted in previous chapters of this guide, there are also new ways of blocking this, for example through censorship, filtering of search results, or surveillance tools that can have a chilling effect on speech. In some cases, governments and others simply shut down the internet in order to prevent

communication. Even in the most totalitarian regimes of the past, it was not possible to prevent words leaving someone's mouth, yet that is the case with online expression today.

Clearly, of course, there are some situations where free expression is unacceptable, for example when it serves to provoke violence or constitutes criminal activity. Yet there needs to be a proportionate approach to these cases, which focuses on illegal activities, while minimising damage to the rights of others.

Fortunately, there is also a strong community of NGOs advocating for action in favour of this freedom, not least Access Now, Article 19, the Association for Progressive Communications, and Freedom House, which produces the annual Freedom of the Net report.

Adapting Existing Rights to a Digital Age: Right to a Private Life

Another example of a pre-existing right is that to a private life. It covers the right to live without interference or intrusion, and is recognised as a key means of allowing individuals to fulfil their potential and live in peace. Clearly, like free speech, there are potential limitations to this, as, for example, has been established in cases concerning the freedom of the press.

As with freedom of expression, the internet has accentuated a pre-existing debate. Individuals – the beneficiaries of the right – have long surrendered some measure of privacy to governments and others. Governments have gathered data and exercised control in order to deliver public services (such as health) and public goods (such as security). Businesses also have collected information about customers in order to target sales and build loyalty.

However, the internet has transformed this. The volumes of data that can be collected allow those with the possibility to gain unprecedented insights into behaviours and preferences. This is the model of services such as Google and Facebook, who offer a free service in exchange for data which can be used to create high-value advertising. It is debatable whether those using these services always know that potentially very personal data is being exchanged in this way.

Moreover, the fact of collecting this sort of data creates the possibility of breaches, with other individuals, companies or even governments looking to steal data, either in order to compromise users, or steal value. Recent examples from Google and Facebook show that even the biggest firms are vulnerable. Legislation such as the General Data Protection Regulation in the European Union have sought to give individuals new rights to view and control the data companies collect about them.

Government data collection too is growing powerful, raising concerns about the degree of control states can exercise over their citizens. For example, there were many concerns around the Aadhaar programme in India that is seeking to collect, digitally, biometric information about all Indian citizens to allow for identification when using government services. Critics have been worried about its mandatory nature, the risk of information being passed to businesses, and the possibility of data breaches.

Of course, individuals can also compromise each other's privacy, for example through leaking photos or videos. This has been difficult to address sometimes because the law tends to focus on governments and businesses, but there are growing efforts to criminalise those guilty of posting revenge porn online, for example the Video Voyeurism Prevention Act in the United States.

While the question of cross-border protection of human rights will be raised later, it is worth noting one particular application of existing rights in a digital age – the right to be forgotten.

This is the result of the application of existing law to the case of a Spanish national, Mario Costeja Gonzales. Mr Costeja felt that the inclusion of stories about previous bankruptcies in search results for his name constituted an attack on his privacy. While, arguably, these stories continued to exist in newspaper archives, the fact that they could so easily be found by using a search engine meant that Mr Costeja's past was much more visible than would otherwise have been the case.

Counter-arguments included reference to free speech (in particular that of the journalists originally reporting on the judgement), as well as to the risks to library and archive collections of being unable to make content available through search engines.

The court nonetheless decoded in favour of Mr Costeja, and created a principle by which individuals could ask for the delisting of search results which they deemed to be outdated or irrelevant, and so unfairly prejudicial to the individual's privacy. The search engine (and on appeal, the government) would then need to assess the merits of the claim, and take a decision to delist or not. Where this is the case, the original underlying webpage remain online, but will no longer be listed in search results for the individual's name.

It is worth nothing that the EU's General Data Protection Regulation not only introduces the concept of the Right to Be Forgotten into legislation, but also underlines that there can be a right to erase underlying data.

Adapting Existing Rights to a Digital Age: Minority Rights

Following the Universal Declaration of 1948, there have been various efforts to define more clearly the rights of groups most at risk of discrimination or mistreatment. There is, therefore, also a need to establish how these texts apply on the internet.

In the case of the right of children, as with the rest of the population, it is assumed that the internet brings both benefits and risks. The need to ensure freedom of expression and access to information, and to address the risks they might face is in line with the United Nations Conventions of the Rights of the Child. Various tools are available online, such as parental locks or filters, and there are ongoing discussions about how to tackle the potential harms to younger people.

The main international instruments for the protection of women's rights are the 1952 Convention on the Political Rights of Women and the 1979 Convention on the Elimination of All Forms of Discrimination against Women (CEDAW). There is clearly much to do still in the physical world, but in addition, there is a risk that offline gender discrimination can extend into the online world, with examples of harassment and abuse far too common.

Furthermore, there is also a gap in the share of women who are using the internet in the first place, with the worrying reality that, according to ITU data, the gap between men and women in terms of connectivity may be increasing. Both of these factors reduce the potential of the internet as an instrument of empowerment for women, and need to be addressed.

Another group facing the possibility – or reality – of discrimination are people with disabilities. These constitute up to a billion people worldwide, according to the WHO, and are the subject of the 2006 Convention on the Rights of Persons with Disabilities.

For many of them, the Internet means new possibilities for inclusion and social interaction, at least where the appropriate access and frameworks exist to support their needs. Yet to achieve this, there needs to be a strong focus on applying solutions to enable access, for example though tools such as the World Wide Web Consortium's Web Accessibility Initiative.

New Rights: The Right to Connectivity

While the examples given so far focus on the application of existing rights in the digital world, there is also talk of a new right – that of being connected to the internet in the first place.

The internet has proven its potential as a tool for obtaining information, undertaking education, developing communication skills, and achieving a wide range of other goals. As a result, not being able to connect to the Internet and access its wealth of information can limit our ability to learn and develop.

Several countries, such as Estonia and Finland, have therefore made access to the Internet a human right and enacted universal service legislation to guarantee access to all. The World Summit on the Information Society, already in 2005, underlined the importance of everyone being able to benefit from the opportunities created by the internet.

Yet the question is slightly more complicated. There are differences in the quality or scope of connectivity. The debate around net neutrality (and zero rating) illustrates some of the concerns that exist, given that these restrict, or at least strongly influence what people can view when they go online. For example, a zero rating scheme that allows some sites and services to be used without counting towards a users' data cap will tend to turn them away from services for which they would need to pay. In reaction, India, for example, banned all zero-rating schemes in 2016 and approved net neutrality rules that also ban blocking and throttling.

In the context of access to the Internet is important to remember the fundamental role libraries plays worldwide in guaranteeing free access to the for their patrons. IFLA has argued, alongside partners, for public access in libraries as a key means of delivering this new right.

The International Dimension

Traditionally, human rights have very much been enjoyed (or repressed) at the local level, where individuals are active. The fact that different countries take different approaches to rights has been more of a political than a practical question. However, the nature of the internet means that the exercise of rights locally can be affected by actions and conditions far away.

For example, the processing of consumer data may often take place in a different country, or even continent, to the where it was collected. This is the case when US companies provide services to Europeans.

This became complicated because there is a difference in how the EU and US enforce rules around data protection. In Europe, governments are in charge, whereas in the US, there tends to be a stronger focus on self-regulation by companies themselves. This has posed a concern for European legislators, who are worried that US companies may not be protecting EU citizens' data sufficiently.

At first, the impasse was resolved with 'Safe Harbour' privacy principles that were designed to prevent disclosure or losing of personal information of European data when handled in the USA. In 2015, though, the Court of Justice of the European Union invalidated the framework, which was eventually replaced by the Privacy Shield. Nonetheless, in the absence of touch privacy legislation at the federal level in the United States – or elsewhere – questions remain about the effectiveness of EU privacy rules.

A second question is linked to the right to be forgotten, which sits at the cross-roads of free speech, free access to information, and the right to a private life. There is an ongoing discussion about geographical application of decisions.

Crucially, the way in which a judge in one country may determine if a story is still relevant may be different to that in another. However, if Right to be Forgotten judgements are applied universally, the possibility for a judge in another jurisdiction to take a decision is effectively cancelled out. This creates a worrying precedent that could allow a country with particularly tough rules about lèse-majesté or criticism of government figures to force the delisting of results that would be perfectly acceptable elsewhere.