COM6655 Professional Issues

Autumn 2022-23

Data protection, privacy and freedom of information (part 3)

Dr Maria-Cruz Villa-Uriol
Department of Computer Science, University of Sheffield
m.villa-uriol@sheffield.ac.uk

Overview

- Privacy in the computer age
- Three aspects of privacy
- DPA 2018 (Data Protection Act)
- EU GDPR (EU General Data Protection Regulation)
- UK GDPR (UK General Data Protection Regulation)
- Information Commissioner’s Office - ICO
- Investigatory powers
- Summary

UK GDPR rights for individuals

10 rights for individuals

- You have the right to:

1) Be informed if your personal data is being used.
   An organisation must inform you if it is using your personal data.
2) Get copies of your data.
   You have the right to find out if an organisation is using or storing your personal data.
3) Get your data corrected.
   You can challenge the accuracy of personal data held about you by an organisation.
4) Get your data deleted.
   You can ask an organisation to delete personal data that it holds about you.

10 rights for individuals

- You have the right to:

5) Limit how organisations use your data.
   You can limit the way an organisation uses your personal data
6) Data portability.
   You have the right to get your personal data from an organisation in a way that is accessible.
7) Object to the use of your data. You have the right to object to the processing or use of your personal data in some circumstances.
8) Access information from a public body. Make a request for information from a public body.
9) Raise a concern.
   Tell an organisation if you are concerned about how they are using or handling your data.

10 rights for individuals

- Your rights relating to decision being made about you without human involvement:

10) You can request that decisions are not solely based on automated processing if the decision affects your legal rights or equally important matters, to understand the reasons behind those decisions and the possible consequences, and to object to profiling in certain situations, including direct marketing.

Exemptions

- The UK GDPR and DPA 2018 set out exceptions from some of the rights and obligations in some circumstances
- Whether or not applicable, it depends on why the personal data is processed
- It is not recommended to routinely rely on exemptions, and they need to be considered on a case-by-case basis
- Reasons for an exemption need to be documented
- Exemptions in the DPA 2018 can relieve you of obligations for: the right to be informed, the right of access, dealing with other individual rights, reporting personal data breaches, and complying with the principles.
- Typical examples where an exemption is adequate are for domestic purposes, law enforcement, and intelligence services processing
- Immigration exemption and National security and defence exemption

Exemptions

What exemptions are available?

Crime, law and public protection

- Crime and taxation: general
- Crime and taxation: risk assessment
- Information required to be disclosed by law or in connection with legal proceedings
- Legal professional privilege
- Self incrimination
- Disclosure prohibited or restricted by an enactment
- Immigration
- Functions designed to protect the public
- Audit functions
- Bank of England functions

Regulation, parliament and the judiciary

- Regulatory functions relating to legal services, the health service and children's services
- Other regulatory functions
- Parliamentary privilege
- Judicial appointments, independence and proceedings
- Crown honours, dignities and appointments

Journalism, research and archiving

- Journalism, academia, art and literature
- Research and statistics
- Archiving in the public interest

Health, social work, education and child abuse

- Health data – processed by a court
- Health data – an individual's expectations and wishes
- Health data – serious harm
- Health data – restriction of the right of access
- Social work data – processed by a court
- Social work data – an individual's expectations and wishes
- Social work data – serious harm
- Social work data – restriction of the right of access
- Education data – processed by a court
- Education data – serious harm
- Education data – restriction of the right of access
- Child abuse data

Finance, management and negotiations

- Corporate finance
- Management forecasts
- Negotiations

References and exams

- Confidential references
- Exam scripts and exam marks

Subject access requests – information about other people

- Protection of the rights of others

National security and defence

- National security and defence

A longer list of exemptions available from ICO: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/exemptions/#ib4

Data protection rights requests

- Under data protection law there are time limits for responding:
  - Organisations must respond as quickly as possible.
  - No later than one calendar month, starting from the day they receive the request.
  - If the organisation needs additional information, the time limit begins once they have received the requested info.
  - If the request is complex or you make more than one, the response time might be a maximum of three months.

Automated decision making and profiling

- The UK GDPR has provisions on:
  - Automated individual decision-making (making a decision solely by automated means without any human involvement)
  - Profiling (automated processing of personal data to evaluate certain things about an individual). Profiling can be part of an automated decision-making process.

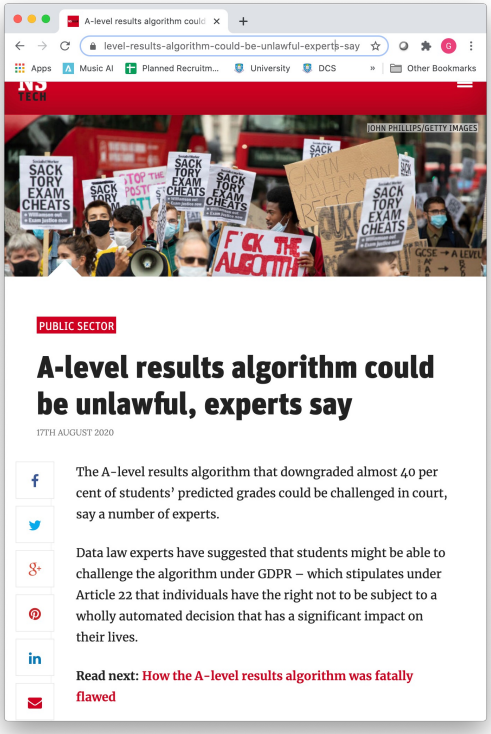
Automated decision making and profiling

- Article 22 has additional rules to protect individuals if you are carrying out solely automated decision making that has legal or similarly significant effects on them.
- You can only carry out this type of decision-making where the decision is:
  - Necessary for the entry into or performance of a contract; or
  - Authorised by domestic law applicable to the controller; or
  - Based on the individual's explicit consent.
- You must identify whether any of your processing falls under Article 22 and, if so, make sure that you:
  - Give individuals information about the processing;
  - Introduce simple ways for them to request human intervention or challenge a decision;
  - Carry out regular checks to make sure that your systems are working as intended.

What are significant effects?

- Automated decisions with legal or similar significant effects include, e.g.
  - Automatic refusal of an online credit application
  - E-recruitment not involving human intervention
  - Loan decisions
  - Access to health services
  - Access to education
  - Online advertising / differential pricing

Example: A-level exams (2020)



PUBLIC SECTOR

A-level results algorithm could be unlawful, experts say

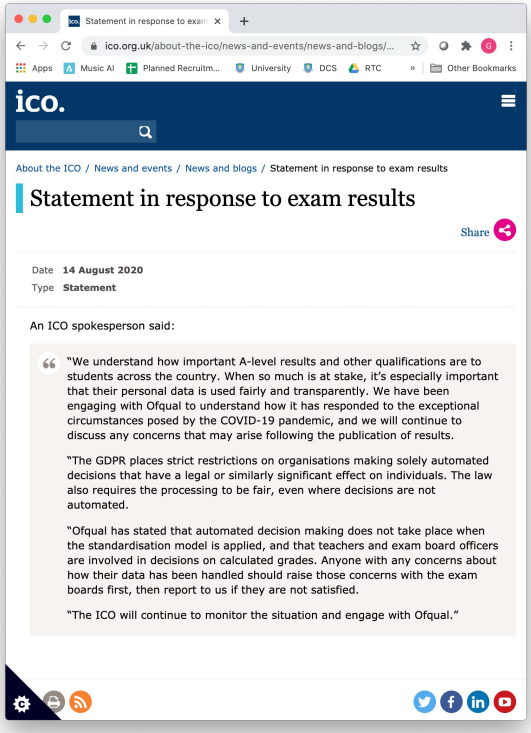
17TH AUGUST 2020

The A-level results algorithm that downgraded almost 40 per cent of students' predicted grades could be challenged in court, say a number of experts.

Data law experts have suggested that students might be able to challenge the algorithm under GDPR – which stipulates under Article 22 that individuals have the right not to be subject to a wholly automated decision that has a significant impact on their lives.

Read next: How the A-level results algorithm was fatally flawed

https://tech.newstatesman.com/public-sector/a-level-results-algorithm-could-be-unlawful-experts-say



About the ICO / News and events / News and blogs / Statement in response to exam results

Statement in response to exam results

Share

Date **14 August 2020**
Type **Statement**

An ICO spokesperson said:

> "We understand how important A-level results and other qualifications are to students across the country. When so much is at stake, it's especially important that their personal data is used fairly and transparently. We have been engaging with Ofqual to understand how it has responded to the exceptional circumstances posed by the COVID-19 pandemic, and we will continue to discuss any concerns that may arise following the publication of results.
>
> "The GDPR places strict restrictions on organisations making solely automated decisions that have a legal or similarly significant effect on individuals. The law also requires the processing to be fair, even where decisions are not automated.
>
> "Ofqual has stated that automated decision making does not take place when the standardisation model is applied, and that teachers and exam board officers are involved in decisions on calculated grades. Anyone with any concerns about how their data has been handled should raise those concerns with the exam boards first, then report to us if they are not satisfied.
>
> "The ICO will continue to monitor the situation and engage with Ofqual."

https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2020/08/statement-in-response-to-exam-results/

Other relevant legislation

- PECR - Privacy and Electronic Communications Regulations (EC Directive 2003) was latest updated on 29 March 2019
- PECR are derived from European law, and it is commonly know as the e-privacy directive
- The EU is currently updating its current directive, which will not automatically form part of UK law
- PECR regulates:
  - Marketing by electronic means, including marketing calls, emails, texts and faxes,
  - Use of cookies (or similar) that track information about people accessing a website or other electronic service
  - Security of public electronic communications services
  - Privacy of customers using communications networks or services as regards traffic and location data, itemised billing, line identification services (eg caller ID) ,and directory listings.

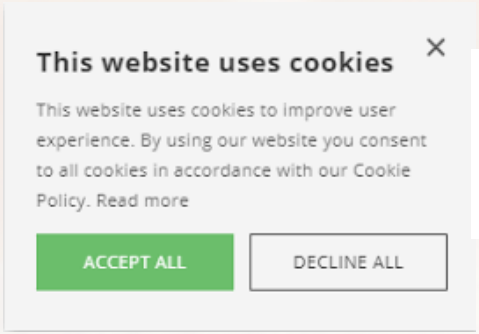
https://ico.org.uk/for-organisations/guide-to-pecr/

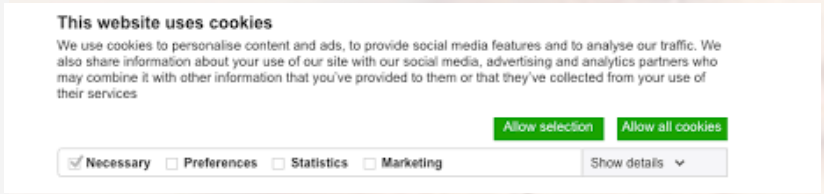
Other relevant legislation

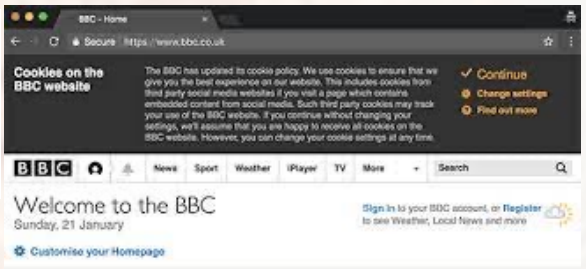
- **For example, email marketing:**
  - sender must not conceal their identity, and must provide a valid opt-out address
  - senders cannot send messages unless they have the recipient's prior consent
  - some exemptions if addresses collected in the course of a sale, or negotiations for a sale

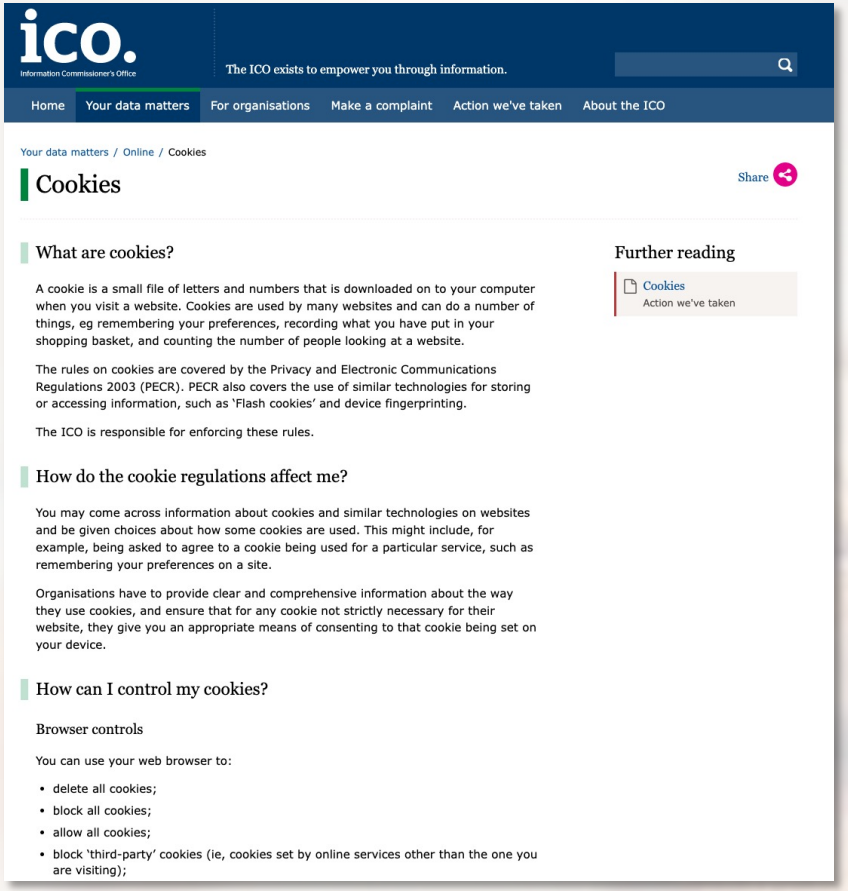
Other relevant legislation

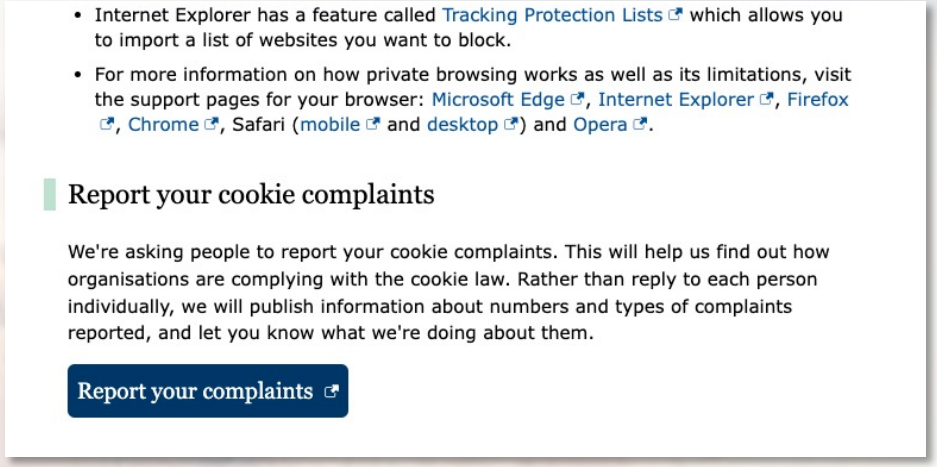
- **Another example, cookies.**
  Basic rule is that you must:
  - tell people the cookies are there;
  - explain what the cookies are doing and why; and
  - get the person's consent to store a cookie on their device.











https://ico.org.uk/your-data-matters/online/cookies/

Information Commissioner's Office - ICO

ICO: The Information Commissioner's Office

- The responsibilities of the Information Commissioner include:
  - Compiling and maintaining a register of persons who hold personal data;
  - Serving notices to those who contravene the Act;
  - Ensuring that requests for information from individuals to persons that hold data about them are honoured.
- The Information Commissioner has a web site: https://ico.org.uk
- The Information commissioner can enforce the Act by
  - Enforcement notices
  - Prosecution under the act

More recent examples

https://ico.org.uk/action-weve-taken/

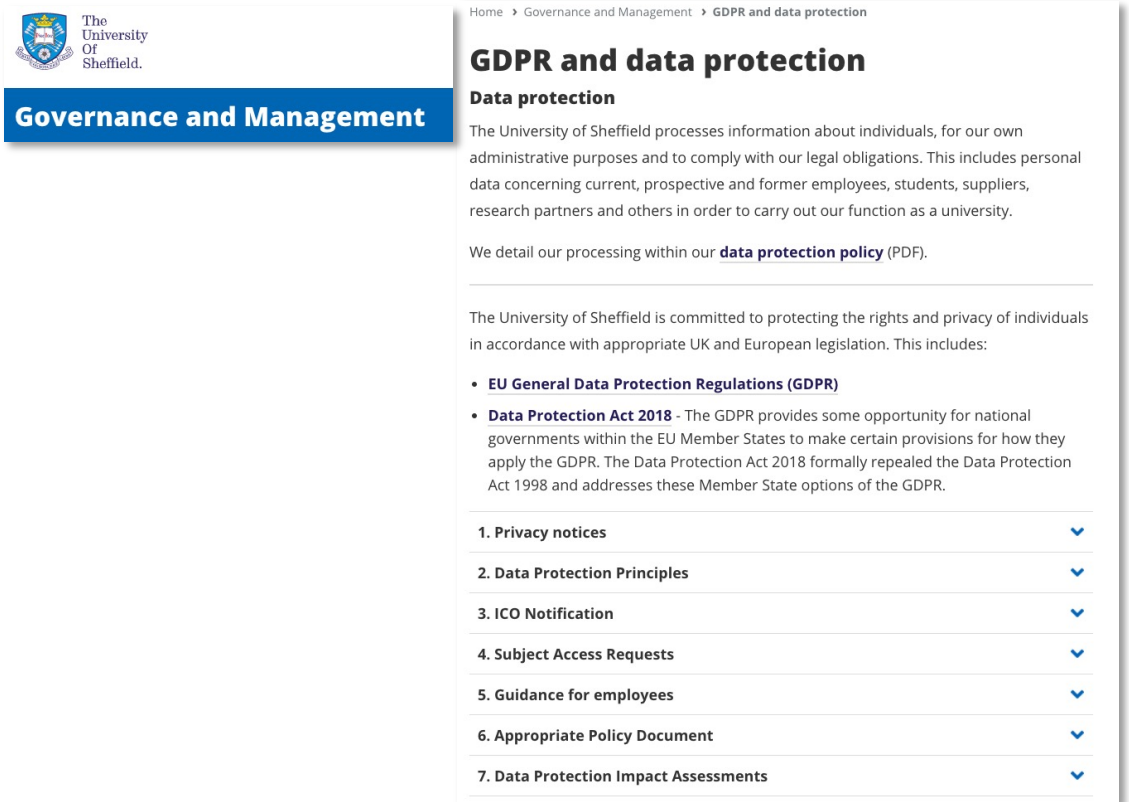
Freedom of Information Act 2000

- Drive for more transparency and ‘open government’. Gives people access to information held by public authorities.
- Right to request public authorities to confirm or deny whether they hold information described in the request
- Similar rights of access to Data Protection Act.
- Also the responsibility of the Information Commissioner.
- Act popular with journalists, but many exemptions, especially for information about government
- In some cases, these requests might have some associated charges (e.g. to cover communication costs)

*Full text available: https://www.legislation.gov.uk/ukpga/2000/36/contents
https://ico.org.uk/for-organisations/guide-to-freedom-of-information/what-is-the-foi-act/

Data protection and the University

https://www.sheffield.ac.uk/govern/data-protection



Investigatory powers

Investigatory Powers

- The Regulation of Investigatory Powers Act 2000 (RIPA) came into force in October 2000.
- Investigatory powers are the powers by which an authorised organisation can covertly gather information for investigative or intelligence purposes including aspects such as:
  - Part I: Interception of communications data
  - Part II: Surveillance
  - Part III: Encryption
- Amended by the Investigatory Powers Act (IPA) 2016*
- Both RIPA 2000 and IPA 2016 are highly controversial

*Full text available here: https://www.legislation.gov.uk/ukpga/2016/25/section/1

RIPA 2000

- There are two distinct sets of powers under the Regulation of Investigatory Powers Act 2000 (RIPA) relating to communications.
  - First, RIPA provides powers to intercept the content of communications, for example, by listening to telephone conversations or voicemail messages (Chapter 1 of Part 1 of the Act). The warrant is signed by the Home Secretary, Foreign Secretary, Northern Ireland Secretary or Scottish Ministers and oversight is provided by Interception of Communications Commissioner.
  - Second is the power to acquire communications data, such as records of who contacted whom, when, from where and for how long (Chapter 2 of Part 1 of the Act). Authorisations for the acquisition and disclosure of communications data are issued by 'designated persons' within the organisations seeking the data, for instance a Superintendent in a police force …

https://publications.parliament.uk/pa/cm201415/cmselect/cmhaff/711/711.pdf

RIPA: What it means

- Certain public bodies may conduct surveillance and access a person's electronic communications in bulk:
  - Demand that an Internet Service Provider (ISP) provide access to a customer's communications in secret;
  - Mass surveillance of communications in transit;
  - Demand ISPs fit equipment to facilitate surveillance;
  - Demand that someone hand over keys to protected information;
  - Monitor people's Internet activities;
  - Prevents the existence of interception warrants and any data collected with them from being revealed in court.

Differing opinions

- “In updating law enforcement powers, we have been careful to see that individuals' rights are properly protected. This is all about a balance. We believe that RIPA strikes the right one.”
  - Jack Straw, UK Home Secretary, 2000

- "Jack Straw has reversed the usual burden of guilt: all encrypted files on your computer are presumed to be incriminating unless you can prove otherwise. Oh, and if you make any public complaint about your treatment, another five years will be added to the sentence. Only a home secretary as ingenious as Straw could invent a new crime of forgetting one's password..."
  - The Guardian (Francis Wheen, May 2000)

https://www.fipr.org/rip/

Investigatory Powers Act (2016)

- A Bill to make provision about the interception of communications, equipment interference and the acquisition and retention of communications data, bulk personal datasets and other information; to make provision about the treatment of material held as a result of such interception, equipment interference or acquisition or retention; to establish the Investigatory Powers Commissioner and other Judicial Commissioners and make provision about them and other oversight arrangements; to make further provision about investigatory powers and national security; to amend sections 3 and 5 of the Intelligence Services Act 1994; and for connected purposes.

- https://services.parliament.uk/bills/2015-16/investigatorypowers.html

Investigatory Powers Act (2016)

- "It legalises a whole range of tools for snooping and hacking by the security services unmatched by any other country in western Europe or even the US." (Guardian, November 19th 2016)
- The legislation sets out clearly for the first time the surveillance powers available to the intelligence services and the police.
- It legalises hacking by the security agencies into computers and mobile phones and allows them access to masses of stored personal data, even if the person under scrutiny is not suspected of any wrongdoing.

A snoopers' charter?

- Civil rights and privacy campaigners called the 2016 Act a "snoopers charter"
- These Acts may be overused: is this a threat to civil liberty?
  - In 2008 RIPA was used to justify putting three children and parents under surveillance in Dorset to check whether they lived in the school catchment area.
  - Other councils have used surveillance to catch dog fouling*, or fly tipping**.

*dog fouling → being in charge of a dog and failing to remove the faeces after it defecates in a public place
** fly tipping → illegal dumping of waste

Objections

- Author and journalist Heather Brooke wrote in The Guardian:
  - “The spies have gone further than [George Orwell] could have imagined, creating in secret and without democratic authorisation the ultimate panopticon. Now they hope the British public will make it legitimate.” (Guardian, 2015)
- Edward Snowden tweeted:
  - “By my read, #SnoopersCharter [The Draft Investigatory Powers Bill] legitimises mass surveillance. It is the most intrusive and least accountable surveillance regime in the West.”

- Source: ComputerWorldUK November 11 2015, Scott Carey

Legal challenges

- The organization Liberty has led legal challenges to the Investigatory Powers Act
- Most recently, challenged whether the Act is compatible with the European Convention on Human Rights
  - Article VI: Everyone charged with a criminal offence shall be presumed innocent until proved guilty according to law.
  - Article VIII: Everyone has the right to respect for his private and family life, his home and his correspondence.
- Legal challenge was unsuccessful: deemed that sufficient safeguards are in place in the Act.
- https://homeofficemedia.blog.gov.uk/2019/07/29/judgment-in-investigatory-powers-legal-challenge/

Summary

- Governments must find a fair balance between respecting privacy and the freedom of information.
- Data Protection Act 1998 enforced the principle that every individual should have the right to know what information is stored about him or her on computer, and the purpose for which it is used.
  - DPA 1998 was first replaced by EU GDPR and UK Data Protection Act 2018
  - After the Brexit transition period, personal data processing is regulated by the UK GPDR and DPA 2018
  - UK GDPR maintains the EU GPDR principles, and mostly affects transborder data transfers
  - The DPA 2018 imposes obligations on data usage, and provides access rights to individuals.
  - Differences to earlier DPA - greater emphasis on transparency
- Freedom of Information Act 2000: access to information held by public authorities.
- RIPA 2000 and the Investigatory Powers Act 2016 provide a statutory framework for surveillance, including 'interception' of data communications via an ISP. It is highly controversial.