Is the Regulation of Investigatory Powers Act (RIPA) 2000 too far out of date to keep up with the advancing technology Police are dealing with? Discuss.

RIPA 2000

RIPA Act 2000 is the primary piece of legislation today for surveillance, interception of communications;

(1) It shall be an offence for a person intentionally and without lawful authority to intercept, at any place in the United Kingdom, any communication in the course of its transmission by means of –
(a) a public postal service; or
(b) a public telecommunication system.

Evident by the definition, when this law was passed, the postal service and public telecommunication system were perceived as the primary means of communication.
The wording of this law has caused significant issues and potential loop holes; 'in the course of its transmission'. – in today's society you cannot intercept voicemails and other means of communication lawfully.
Example – celebrity phone hacking scandal.

Cases:

Liam Allan (22) – Metropolitan Police wrongly accused Liam and charged him with 12 counts of rape and sexual assault. The Police failed to review the 57,000 text messages properly which had evidence that the alleged victim had actually been pestering him for sex.

Celebrity phone hacking - the media and newspaper reporters hacked into celebrities phones and disclosed their private lives. Due to the definition and the loop holes, the media could not be prosecuted and the cases were settled by voluntarily compensating the victims.

What issues have arisen due to the archaic act:

Disclosure:
- In 2000, technology, mainly mobile phones could store very little data.
- Today, storage has expanded exponentially. (Comparison of a Nokia in 1995 to the new IPhone X which has 256 GB).
- Police can now download tens of thousands of pages of data.

- How is it managed from a disclosure perspective?
- How do the Police review and sift through all the data?
- Proportionality: what is the timeframe they can look back on?
- Does disclosure allow pitfalls for the defence solicitors to undermine the case? (If the Police only focus on a little bit of data, the defence argue they have been too selective. If they review everything, the defence criticise the police for a draconian infringement of privacy).
- Do the Police have the time and resources for every case? (Potentially desirable to cut corners).

- Disclosure is governed by the Criminal Procedure Investigations Act 1996 – duty to retain, record and reveal material.
- It is arguable that this law needs updating to allow the Police to carry out investigations effectively in a timely manner. Additionally reducing pitfalls.

Privacy:
- *De facto* electronic tagging of everyone who carries a smart mobile phone.
- Searching a house prior to arrest – court search warrant
- Searching a house after arrest under section 18 – inspectors authority
- Both processes have inbuilt checks and balances.
- Section 19 PACE 1984 allows, with valid reason, a phone to be ceased and searched without a search warrant or safeguards in place.
- Smart phones today reveal more than a house search, giving the Police access to banking and purchasing history, relationship details, messages, calls, photos, Facebook, Instagram and Twitter history, and GPS (location history).

Evolution of Technology:
Technology is advancing year on year at a rate the Police cannot keep up on. It could be argued that training is also a factor of failings alongside Laws.

Conclusion:

RIPA Act 2000 is the primary legislation in relation to surveillance and intercepting communication, however owing to the archaic nature of the act, it does not reflect the advancing technology Police are dealing with. This is demonstrated by the Liam Allan rape case where the Police were unable to monitor all of the text messages, and the celebrity phone hacking case where the Act could not support the prosecution of the media. Disclosure, privacy and evolution of technology are issues which have been linked to the archaic Act. Additionally, the legislation breaches articles within the Universal Declaration of Human Rights.

Breaches of Universal Declaration of Human Rights

- Article 5, Freedom from torture and degrading treatment:
Nobody has the right to torture, harm or humiliate you.

- Article 7, Right to equality before the law:
You have a right to be protected and treated equally by the law without discrimination of any kind.

- Article 8, Right to remedy by capable judges:
if your legal rights are violated, you have the right to fair and capable judges to uphold your rights.

- Article 10, Right to a fair public hearing:
If you are accused of a crime, you have the right to a fair and public hearing.

- Article 11, Right to be considered innocent until proven guilty:
1) You should be considered innocent until it can be proved in a fair trial that you are guilty. (implying fair trail)
2) You cannot be punished for doing something that was not considered a crime at the time you did it.

References:
BBC (2018) *Met Police Apologise for Liam Allan Rape Case Errors.* Available from http://www.bbc.co.uk/news/uk-england-42873618 [accessed 22nd April 2018].
Home Office (2015) *Regulation of Investigatory Powers Act.* Available from https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/417958/DSO_2-2015_RIPA.pdf. [accessed 22nd April 2018].
The Guardian (2015) *Daily Mirror Owners Must Pay £1.2 million to Celebrity Phone-Hacking Victims.* Available from https://www.theguardian.com/media/2015/may/21/daily-mirror-owners-ordered-to-pay-1-2m-to-celebrity-phone-hacking-victims. [accessed 22nd April 2018].
United Nations (1948) *Universal Declaration of United Nations.* Available from http://www.un.org/en/universal-declaration-human-rights/. [accessed 22nd April 2018].