Post-Brexit will EU Data Protection Law Still Impact on Police Investigations into Terrorism and Organised Crime?

by Dr David Lowe

Introduction

January 2021 saw a total break of the UK from the European Union (EU). In post-Brexit UK terrorism and organised crime investigations two factors changed. One is the UK is longer part of the EU's policing agency Europol and consequently has no access to the terrorism/crime intelligence data, along with the fact that the UK no longer can access the European Arrest Warrant (EAW). Secondly the Court of Justice of the European Union CJEU no longer has jurisdiction over UK policing investigations to determine if their actions or the legislation they rely upon violates the EU's Charter of Fundamental Rights and Freedoms (CFRF), or do they? Terrorists and organised crime gangs do not recognise or respect geographical borders and with the UK still being part of continental Europe, a degree of co-operation will still have to exist with EU member states. Focusing primarily on the police gathering of evidence via their powers related to the surveillance of electronic communications, this article will examine the legal implications of intelligence and evidence sharing between UK and EU member states' policing agencies.

The Current Operational Situation Between the UK and the EU

While an EU member state, UK policing agencies had access to EU's policing agency Europol, including its European Counter Terrorism Centre that focuses on:

1. Providing operational support upon a request from an EU member state for investigations;
2. Tackling foreign fighters;
3. Sharing intelligence and expertise on terrorism financing;
4. Dealing with terrorist propaganda and extremism;
5. Dealing with illegal arms trafficking;
6. International co-operation among counter-terrorism authorities.

Due to the UK's Joint Terrorism Analysis Centre (JTAC), this does not mean the UK suffered a major loss in its ability to investigate and counter terrorist activity. Established in 2003 and based at MI5's headquarters at Thames House (although not part of MI5), JTAC analyses and assess all intelligence relating to terrorist activity. It brings together counter-terrorism expertise from the police, the security services and governmental departments and agencies so information is analysed and processed in a shared basis to assess the nature and extent of the terrorist threat to the UK. Using this system, between 2017-2020 UK counter-terrorism agencies foiled 25 terrorism plots in the UK and this included passing on intelligence that foiled four terrorist plots in other EU member states in 2018. Although the UK would now come under working with the European Counter Terrorism Centre under international co-operation, this is not the same as being part of it, especially in relation to immediacy in intelligence sharing and support.

Also, as an EU member state, the UK had access to the EU's database Schengen Information System II (SIS) where, under law enforcement co-operation, SIS allows member states' policing agencies to:

1. Share biometric information such as DNA, facial images and fingerprints;
2. Share information on persons and objects involved in terrorism related activities;
3. Share information related to organised crime.

Perhaps one of the biggest losses of the UK becoming a 'third country' post-Brexit is losing access to the EAW. The EU's EAW is a rapid form of extradition that takes on average between 14 to 17 days compared to the average of just over a year with traditional extradition treaties. The UK was a prolific user of EAW's and it was not just one-way usage. In relation to the EAW, the UK assisted many EU member states' investigations, a process that was beneficial to both UK and EU member states policing agencies. At the time of writing (January 2021) there is a degree of optimism that a separate agreement will be made producing a variant of the EAW for use between the UK and the EU. While Brexit has created new trade agreements and borders, Brexit means little to terrorists and criminals, who as stated, do not recognise state borders and the UK will still have to work with their EU member state partners, none more so than between the UK and the Republic of Ireland were An Garda Siochana constantly work closely with the Police Service of Northern Ireland. This is an important issue as post-Brexit UK policing agencies will still have to co-operate with EU member state policing agencies.

Intelligence and Evidence Gathering via Surveillance of Communications

In the UK intelligence and evidence gathering during police investigations is acquired through various methods ranging from the traditional static and mobile surveillance, which is governed as directed surveillance and intrusive surveillance under sections

27 and 32 of the Regulation of Investigatory Powers Act 2000 (RIPA) respectively. Another method is in the use of covert human intelligence sources, commonly referred to as informants, which is governed by section 29 RIPA. Currently the law in the use of informants is changing with the introduction of the Covert Human Intelligence Resources (Criminal Conduct) Bill that at the time of writing is at its third reading in the House of Lords. When reading the law governing the use of these powers one can see the influence of the European Convention on Human Rights (ECHR) as serious consideration is given to various human rights when granting authorities to the police.

Similar consideration is seen in the UK's Investigatory Powers Act 2016 that grants the police and security services (and where applicable the military, Her Majesty's Revenue and Customs, and, Border Agency) powers to obtain targeted interceptions warrants, warrants to obtain and retain communications data, bulk interception warrants and bulk interference warrants (lawful hacking of communications devices). Globally the use of electronic communications in society has grown exponentially, more so during the COVID-19 pandemic with the expansion in the use of online meetings facilities such as Zoom and Microsoft Teams, shopping and banking online. It is not just legitimate use of the various forms of communication that has expanded, both terrorists and organised crime gangs use and exploit electronic communications, especially in the use of deeply encrypted forms of communication. As such, powers granting policing agencies (including the security services) access to unlawful use of electronic communications is necessary, provided those powers are balanced with consideration of the protection of human rights such as rights to privacy and data protection. In the 2016 Act again we see the ECHR influence in the granting of these intrusive powers provided they are balanced with protecting relevant human rights. The authorities to interfere with these rights are only granted on the grounds of necessity, that is where it is under an act prescribed by law and necessary in a democratic society under certain grounds. These grounds include:

1. the interests of national security (this ground is certainly relevant to terrorism investigations);
2. the prevention of disorder or crime;
3. public safety; and
4. the protection of rights and freedom of others.

In relation to terrorist investigations the protection of the rights and freedom of others will include the right to life (article 2 ECHR), hence why intrusive investigative powers into the lives of citizens are necessary in order to prevent attacks from taking place. It is not only ECHR provisions we see in relation to the protection of rights, there is consideration of the EU's CFRF and two important CJEU case decisions influenced the drafting of the statutes. The relevance of this is with the UK being a third country, its law must be adequate in relation to the protection of human rights, as legislation like the Investigatory Powers Act was introduced while an EU member state, this Act will meet that criteria.

Digital Rights and Tele 2 Cases

Digital Rights: The 2006 Directive on Retention and Access to Communications Data and the Data Retention and Investigatory Powers Act 2015

In *Digital Rights* ([2014] 3 WLR 1607) the CJEU examined the now repealed Directive 2006/24/EC that laid down an obligation on publicly available electronic communications services or public communications networks to retain certain data generated or processed by them. As the Directive allowed EU member states' intelligence and policing agencies to collect bulk data, the CJEU examined the acceptable limits of mass surveillance and the function of data protection in relation to compatibility with articles 7 (respect for private and family life) and 8 (protection of personal data) CFRF. The CJEU declared that the 2006 Directive was invalid on two important legal issues saying to ensure personal data is protected:

1. EU legislation must lay down clear and precise rules governing the scope and application of the measure in question;
2. Minimum safeguards are imposed to provide sufficient guarantees effectively protecting personal data against the risk of abuse and against unlawful access and use.

Under the 2006 Directive member states could retain bulk and personal data only when it was necessary and proportionate to do so. The CJEU held this phrase lacked the required specificity to allow lawful interference with that data and did not place a high enough level of protection of personal data, nor did it ensure there was an irreversible destruction of the data at the end of the data retention period. In *Digital Rights* the CJEU acknowledged data retention is an important strand in terrorism and serious crime investigations to ensure public safety and stated these specific grounds could be a justification. Article 52 allows for limitations in the exercise of CFRF rights where, subject to proportionality, limitations can only be made where they are necessary and genuinely meet the objectives of general interest recognised by the EU. The CJEU held the retention of telecommunications data to allow competent national authorities to have possible access must satisfy an objective of general interest under article 52 CFRF but added in doing so it is necessary to verify the proportionality of the interference found to exist.

It was the latter point on proportionality where the 2006 Directive failed as the CJEU found it was too broad as to the conditions and requirements as to why telecommunications data had to be retained and regarding access to it by competent authorities. As the retention included persons' personal data who had not nor were suspected of being involved in any form of criminal or terrorist activity, the retention of the

data was being carried out in an indiscriminate manner. The requirement under member state law that telecommunications data be retained by communications and internet service providers, it is essential the requirement to do so has to be for specific reasons, that includes defining what is meant by serious crime and disclosure/access to the data has to be necessary to assist in achieving the aim of an investigation and it must be proportionate. As a result of *Digital Rights* many member states repealed their domestic legislation governing the surveillance of electronic communications and retention of telecommunications data. This included the UK. It repealed the provisions in RIPA and introduced the Data Retention and Investigatory Powers Act 2015 (DRIPA) that was drafted with consideration to the *Digital Rights* decision, but in R *(on the application of Davis and others) v Secretary of State for the Home Department and others* ([2015] EWHC 2092 (Admin)) the UK's High Court held that DRIPA did not comply with the decision in *Digital Rights*. The Court held that DRIPA did not lay down clear and precise rules regarding the access and use of communications data, and, on safeguards, the Court held that judicial approval was important to ensure surveillance authorities are not abused in order to protect citizens' rights.

Tele2 and Directive on Privacy and Electronic Communication 2002/58/EC

In *Tele2 Sverige AB*, now referred to as *Tele2* (2016] All ER (D) 107) the CJEU were requested to provide a primary ruling on the interpretation of Article 15(1) Electronic Communications Directive 2002/58/EC concerning e-privacy and electronic communications and its compatibility with Member States' national law regarding the retention and access to telecommunications data. In the full title of the case it included the Davis case heard at the High Court mentioned above that was referred to the CJEU. In *Tele 2* the CJEU examined citizens' rights under the CFRF, mainly articles 7, 8, and 52.

The aim of the 2002 e-Privacy Directive is to protect fundamental rights and freedom in relation to privacy when processing personal data in electronic communications, thereby ensuring the free movement of that data and electronic communications and services in the EU, especially in relation to the protection of subscribers to communications companies' services because in EU law subscribers are legal persons. The Directive is clear that its provisions shall not apply to activities concerning:

> '…public security, defence, State security (including the economic well-being of the State when the activities relate to State security matters) and the activities of the State in areas of criminal law.'

Article 5 states that member states must ensure the confidentiality of communications, including related traffic data by means of a public communications network and publicly available electronic services through their national legislation. This includes the prohibition of listening, tapping, storage or other kinds of interception or surveillance of communications and related traffic data by persons other than the users without the consent of the users concerned. Article 5 contains an exception to this where such activity is legally authorised in accordance with article 15(1) of the 2002 Directive. Article 15(1) allows member states to legislate to restrict the privacy, rights and freedoms related to electronic communications when it is a:

> '…necessary, appropriate and proportionate measure within a democratic society to safeguard national security (i.e. state security), defence, public security, and the prevention, investigation, detection and prosecution of criminal offences…'

In *Tele2* the CJEU pointed out these restrictions laid down in member states' national legislation to privacy only apply only if the member states adopt and meet all the conditions laid down in the Directive. Although recognising that fighting serious crime, especially organised crime and terrorism, depends to a great extent on the use of modern investigation techniques where telecommunications data evidence can be effective, the CJEU added:

> '…such an objective of general interest, however fundamental it may be, cannot in itself justify that national legislation providing for the general interest and indiscriminate retention of all traffic and location data should be considered to be necessary for the purposes of that fight.'

While acknowledging the importance the role the retention of telecommunications data plays in the fight against serious crime, the CJEU's guidance in relation to this matter is it should be read in light of articles 7, 8, 11 and 52(1) CFRF by adopting legislation permitting as a preventative measure targeted retention of traffic and location data for the purpose of fighting crime. The important points in article 52(1) that must be considered are:

1. The limitation of the exercise of rights and freedoms must be provided for by law; and
2. The limitations must be subject to the principles of proportionality; and
3. The limitations must be necessary; and
4. The limitations must meet the general interest recognised by the EU.

The CJEU added the retention of the data must be limited to the categories for data to be retained, the means of communication affected, the persons concerned, and the retention period adopted, with all limitations being strictly necessary.

Conclusion: Current Impact of CJEU Decisions and EU Law on the UK

In relation to the surveillance of electronic communications, the UK's Investigatory Powers Act 2016 took cognizance of the CJEU's decisions in both *Digital Rights* and *Tele2,* as well as the High Court de-

cision in R (*on the application of Davis and others)*. Throughout the Act it consistently states the granting of authorities must be proportionate and necessary with the general interest being to allow relevant state agencies to interfere with those rights on the grounds:

1. of the interests of national security;
2. to prevent or detect serious crime; or,
3. in the interests of the economic well-being of the UK when those interests are relevant to the interests of national security.

It is clear the general interest covered in the Act relates to serious criminal and terrorist activity. Being a third country, this is important as in *Maximillian Schrems v Data Protection Commissioner* ([2014] IEHC 310) the CJEU held when dealing with third countries the EU must ensure there are adequate levels of data protection and privacy rights. The CJEU added this is an ongoing obligation to ensure there are no changes made by the third country and the EU Commission has a duty to regularly review a third country's level of protection. Unlike many other third countries the EU deal with, like the EU's member states, the UK is a signatory to the ECHR that is enshrined into UK law through the Human Rights Act 1998. Under this Act the UK public authorities must act in a way and its statutes are compatible with the ECHR, thereby ensuring another adequate level of protection of human rights.

In relation to intelligence and evidence gathering this is important as on matters of serious organised crime and terrorism, the UK will still have to work in co-operation with EU member states. While it is submitted that the UK's current legislation relating to investigations into these activities provide more than adequate levels of human rights protection, in fact they could be seen as comparable, it will be future legislation introduced by the UK Parliament that could be a cause for concern. This returns us to the question raised at the beginning of this article, would CJEU have jurisdiction on UK law? While the CJEU would not have jurisdiction, its decisions could have an impact on future UK/EU policing agencies co-operation as seen in the *Schrems* decision that brought an end to the EU-US Harbour Agreement (although following that decision an new agreement was quickly drafted and agreed on). Returning to the point that organised crime gangs and terrorists have no respect for borders, the UK is a major player in investigations into this activity and it is not one-way activity with the UK solely benefiting from the EU, the 27 EU member states also benefit from UK co-operation. It is on this point there is optimism an agreement will be made in relation policing co-operation and that on these matters the UK Parliament will ensure that any future legislation governing policing activity will provide adequate protection of rights acceptable to the EU.

About the author

Dr David Lowe is a retired police officer and now a senior research fellow at Leeds Law School, Leeds Beckett University where he researches terrorism & security, policing and criminal law. His research has been widely published in books and journals, including his book Terrorism: Law and Policy published by Routledge in 2018 (a comparative study between the law in Australia, Canada, the EU, New Zealand, the UK and the US), 'Data Protection and Rights to Privacy Involved in Intelligence Gathering and International Intelligence Exchange' in Roberson (editor) Routledge Handbook on Social Justice published in 2018, 'Surveillance of Electronic Communications and the Law' in Morley, Turner, Corteen and Taylor (editors) A companion to state power, liberties and rights, published by Policy Press in 2017 and 'Surveillance and International Terrorism Intelligence Exchange: Balancing the Interests of National Security and Individual Liberty', published in Terrorism & Political Violence in 2016. He has provided expert witness services on several occasions to prosecution and defence teams on police investigations, including the surveillance of electronic communications.