AN CHÚIRT UACHTARACH
THE SUPREME COURT

Clarke CJ
O'Donnell J
McKechnie J
MacMenamin J
Charleton J
O'Malley J
Irvine J

Supreme Court appeal number: S:AP:IE:2019:000018

[2020] IESC 000

High Court record number 2015/351P

[2019] IEHC 685

Central Criminal Court bill number: 2015 No. 351 P

BETWEEN

GRAHAM DWYER

PLAINTIFF/RESPONDENT

- AND -

THE COMMISSIONER OF AN GARDA SÍOCHÁNA, THE MINISTER FOR COMMUNICATIONS, ENERGY AND NATURAL RESOURCES, IRELAND AND THE ATTORNEY GENERAL

DEFENDANT/APPELLANT

Dissent of Mr Justice Peter Charleton delivered on Monday 24 February 2020

Protection of data

1. Ireland has always been concerned with and has given the highest measure of protection to data derived from telecommunications. In 1983, postal and telecommunications services, then a State monopoly, were divested from the Department of Posts and Telegraphs and two new postal and telecoms companies were set up, the latter now privatised. Section 98 of the Postal and Telecommunications Services Act 1983 made it an offence to intercept or reveal telecommunications data. This crime carries a prison term of up to five years and a substantial fine under s 4 of the Act. Under modern legislation, processing tends to be the concept that describes interference with data. In the 1983 Act, s 98 has a complete prohibition, subject to limited exceptions, against the interception of any data. This is defined as including not only "acquiring the substance or purport" of any telecommunications message without the agreement of the parties, but also criminalises disclosing "the existence" of any data or the "substance or purport of any such message" or using any such information in any way. Statutory instrument 517 of 1997 and several other measures require service providers to keep data secure and to erase data when retention of data is not required to be kept by law.

2. Section 13 of the Interception of Postal Packets and Telecommunications Messages (Regulation) Act 1993 inserts s 2A into the 1983 Act and enables an exemption from the criminal offence of disclosure where that is done: (a) with the consent of both parties to the communication; (b) "for the prevention or detection of crime or for the purpose of any criminal proceedings"; (c) "in the interests of the security of the State"; (d) where there

is a court order; (e) for civil proceedings, requiring a court order of discovery; and (f) an exception related to an employee having a duty. A request must be made by a chief superintendent of the police and this must be in writing. Before any data, for instance stating that mobile phone A contacted mobile phone B at a particular time for so many seconds and was routed off a mobile phone mast in a particular part of the city, can be admitted in court, the legality of that request must be proven before the court. That duty is on the prosecution whether challenged by the defence or not, unless formally admitted - which is unlikely. Hence, in a criminal prosecution, the Director of Public Prosecutions is under a duty to the court to show the legality of a measure which involves an exception to the general prohibition. This is the method of obtaining metadata from stored records and it is to be noted that this is not challenged in this case as being invalid as a matter of Irish law. It is a legislative measure for the detection and prevention of crime. That law is not dependent upon the validity of the later Directive no 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks or of the Communications (Retention of Data) Act 2011. The lawful method of accessing data is as in the 1993 Act as amended. Actual listening or real-time interception requires the prior authorisation of a High Court judge.

3. What is concerned here is a criminal prosecution. Part 7 of the Criminal Justice (Terrorist Offences) Act 2005, s 63 which is still in force, requires data to be kept for 3 years in an inert form. Prior to that, under s 110(1)(b) of the 1983 Act, preservation was provided for by direction of the Minister and was accompanied by a requirement to strictly preserve the data. Data is rendered inert by storage. Normally data is stored on hard drives for current use but data on communications, metadata, is shifted off servers and back-up computers onto spools of tape. This is a practical measure but also adds extra security. The tape must be retrieved and run on a computer for metadata from a year or 18 months prior to be recovered. This is part of the security of the metadata and is also done for practical purposes related to the burden of the data if retained live on computer systems of servers. The level of security is thus much higher than is the case with live systems that, theoretically at least, might be hacked into. It will also be observed as regards the strict limitation on time, that retention of inert data has reduced by legislative provisions from 5 to 3 to 2 years.

Utility of data in serious criminal cases

4. Two cases will illustrate the utility of recovering such tapes and running a limited search in respect of particular mobile phones or other telecommunications for criminal prosecutions. In June 1996 a distinguished journalist was shot several times and murdered while stopped in broad daylight at traffic lights near Dublin city. She had been tracked by a spotter from Naas and then followed on her journey on the dual carriageway from there to Dublin. The perpetrators were involved with a Dublin gang which imported drugs and firearms, including sub-machine guns. Of the main participants in the importation gang, of which there were seven, one was ex-Army and had no convictions or reason to suspect him, another was running a shipping company in Cork and there was no

reason to suspect him, another was unemployed and had no convictions. Of the four remaining there were convictions for other offences, some serious, but no current reason for police to suspect them. The journalist had enquired into the gang and its leader in the tradition of courageous investigation in the public interest.

5. Some members of the gang gave evidence relating to the murder and were put into witness protection programs abroad because of justified fears of retribution. Getting such cooperation took several months of painstaking work. But as accomplices, in some respect in the overall criminal enterprise, their evidence was to be regarded with extreme caution by a court. One witness from within the gang, who was a money exporter for it and who had no convictions, described being tasked to go to Naas and to look for a particular red car and report back. This car belonged to the victim. Metadata confirmed a call at that time to another member of the criminal gang. Once the car was on its way to Dublin, metadata relating to calls about spotting the car and reporting back confirmed the evidence. These facts are taken from the relevant judgments of the Special Criminal Court and from appellate judgments, as are the facts following. In both cases, this member of the court was then the prosecutor.

6. On 15 August 1998 in Omagh, Northern Ireland, a bomb was exploded by terrorists killing 29 people, one of whom was a lady pregnant with twins. There was a painstaking investigation which lasted many months. The mobile phone of a person accused of conspiring to perpetrate the bombing was analysed and its metadata was recovered pursuant to the safeguards under Irish and British legislation. The mobile phone of an uninvolved man was 'borrowed' for purposes which, according to the main suspect, that individual was completely unaware of. This uninvolved man, as with three of those involved in the gang in the prior paragraph, had no convictions and there was no reason to suspect him or keep him under any form of surveillance. On a pretext of the suspect's mobile phone needing repair, it was borrowed for the duration of a weekend. The metadata showed the two phones communicating with each other in a pattern of calls of short duration from Dundalk to Omagh, some 110km, and returning from Omagh to Dundalk. Whereas because the suspect and the person whose phone was borrowed on a pretext worked together, there might be reason for them to contact each other for innocent purposes, analysis gave no reason for this kind of pattern where the phones utilised masts up and down in a northwest and then southeast pattern at a weekend. The calls were routed through fixed masts as the mobile phones, carried in cars, went on their journey and used different masts in turn, showing a valuable pattern. This was essential to detect and so to deter serious crime. The Special Criminal Court, consisting of three judges of trial from the High Court, the Circuit Court and the District Court, regarded this evidence as central. This is an extract from the judgment, later reversed on appeal on completely unrelated grounds:

> *The pattern of calls and sell-mast user by both phones on [the day of the Omagh bombing] indicate that each travelled from County Monaghan [in a Northerly direction] to Omagh shortly before the detonation of the car bomb there and also returned [in a southward direction to County Monaghan where the accused lived]*

thereafter. It is highly probable that the conveyance of the car-bomb to Omagh that day would have involved, not only the bomb carrying vehicle itself but also a scout car to travel ahead of it. Telephone contact between both vehicles in such circumstances is probable. Contact with the person who gave the bomb warnings may also have been made by the accused's or Morgan's phone.

7. Prior authorisation for inert data storage could not have solved the murders at Omagh and of the journalist. Several suspects were beyond suspicion. As to geographical range, this would involve mere guesses: since two jurisdictions, Ireland and Northern Ireland, and several towns were involved in the Omagh terrorist outrage, and Dublin, Naas, Cork were the random locations that the relevant crime scenes proved to throw up in the other murder case.

Duty to show legality

8. As a matter of Irish criminal law, police powers involving an intrusion into liberty. the home or other fundamental rights require justification in law. Admission of such evidence at trial depends on judicial analysis. These intrusions can only be exercised on the basis of reasonable suspicion. Police or other authorities cannot infringe guaranteed rights as a matter of criminal law without reasonable suspicion. Telecommunications data cannot be accessed without reasonable suspicion and this is part of the proofs in a criminal trial. In *CRH plc v Competition and Consumer Protection Commission* [2017] IESC 34 the law on reasonable suspicion was summarised thus:

> *A reasonable suspicion is one founded on some ground which, if subsequently challenged, will show that the person arresting, issuing the warrant or extending the detention of the accused acted reasonably; see Glanville Williams, "Arrest for Felony at Common Law" [1954] Crim LR 408. A reasonable suspicion can be based on hearsay evidence or the discovery of a false alibi; Hussein v Chong Fook Kam [1970] AC 942: or on information offered by an informer who is adjudged reliable; Lister v Perryman [1870] LR 4 HL 521, Isaacs v Brand (1817) 2 Stark 167, The People (DPP) v Reddan [1995] 3 IR 560. A suspicion communicated to a garda by a superior can be sufficient to constitute a reasonable suspicion, as may a suspicion communicated from one official to another, which is enough to leave that other individual in a state of reasonably suspecting; The People (DPP) v McCaffrey [1986] ILRM 687. The fact that a suspect is later acquitted does not mean that there was not a reasonable suspicion to ground either an arrest or a search. It is accepted by the European Court of Human Rights that "the existence of a reasonable suspicion is to be assessed at the time of issuing the search warrant"; Robathin v Austria [2012] ECHR 30457/06 at para. 46. Having information before a judge of the District Court whereby he or she may reasonably suspect the potential presence of information on a premises founds the warrant.*

Crime as human rights violations

9. Murder, rape and other serious crimes are fundamental violations of human rights, going so far as to remove all human rights by violent death. Article 47 of the Charter of Fundamental Rights of the European Union provides: "Everyone whose rights and

freedoms guaranteed by the law of the Union are violated has the right to an effective remedy before a tribunal in compliance with the conditions laid down in this Article." Experience puts this following proposition beyond any doubt: without the secure retention of metadata and the potential to access and analyse it for strictly limited purposes related criminal investigation, the most serious crime against life and limb would remain undetected. Victims, including the survivors of victims' families, would be deprived of their human right to access a court proceeding in pursuit of justice. Investigators would be shorn of an indispensable tool for detecting human rights violators. Justice must be an energetic search for the truth upon which alone any fair verdict against an accused person or any vindication of human rights violations can be based. Cutting out the truth in the form of useful and convincing evidence leads to the distortion of the legal process and its being severed from the good sense of the European peoples. Criminologists agree that the fear of detection is central to the deterrence of crime. Ireland has suffered, as the two examples given illustrate, from both organised crime and from terrorism. As the examples also elucidate, these threats to society are dampened by a detection approach which is moderate, protective of private rights and which is founded on the certainty of the legal order.

Reasons for dissent

10. There are thus two reasons for dissenting from referring issues to the Court of Justice of the European Union. Firstly, issues of the proportionality of a legislative measure impinging on guaranteed rights should be resolved by the national courts and can therefore be resolved here. The second reason relates to the competence of the Court of Justice of the European Union in criminal litigation. Any issue of *Kompetenz-kompetenz* is not lightly to be engaged whereby this Court should rule on its own and exclusive jurisdiction in the field of criminal law. The duty of sincere cooperation requires an analysis of the extent and limits of national and European Union competence in ruling on the recovery of evidence in criminal cases and the presentation of evidence as part of a criminal prosecution. It is not appropriate to refer cases under Article 267 of the Treaty of the Functioning of the European Union which relate to criminal law and which ought to be resolved by the application of the four stage test on the protection of rights.

Proportionality is a matter for national courts

11. The mobile phones at issue in this case were abandoned by whoever used them. Data analysis at the criminal trial proved that one phone belonged to the accused, and that the other was given by to him by his accused employer. Guns and other weapons are often abandoned in the aftermath of a crime. Where a long-barrelled firearm is found, test firings can establish striations on test bullets and these can be compared to a library of bullets found at the scenes of other crimes. Bullet casings may have distinctive hammer strike marks which can establish a connection as between casings found at the scene of a crime and an abandoned firearm, whether long-barrelled, automatic or short-barrelled. In a similar way, fingerprints, DNA, fibres and other traces at the scene of a crime establish culpability when linked to other evidence. The collection of data and access to data are two sides of the same coin. It cannot be that it is part of European law that collection of data in an inert way and subject to serious criminal sanction for breach of protections, as

provided for in Irish law and practice, offends human rights under the Charter or legislation. If a reasonable suspicion or prior authorisation is first required before there can be any inert collection, there is no need for later authorisation. The reasonable suspicion is already there once the data is collected. Irish law provides for inert collection with access strictly limited on the basis of reasonable suspicion.

12. It is a matter for national courts to resolve any issues of compliance. Certainly under Article 8 of the Charter, everyone has the "right to the protection of personal data concerning him or her" and that same "must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law." This right need not clash with rights to life or bodily integrity guaranteed under Articles 1, 3 and 6 of the Charter since Article 52 provides that any "limitation on the exercise" of any guaranteed right "must be provided for by law and respect the essence of those rights and freedoms." Section 98 of the 1993 Act, s 53 of the 2005 Act and the other guarantees as to inertness and storage in Irish legislation demonstrate such respect. As Article 52 also provides: "Subject to the principle of proportionality, limitations may be made only if they are necessary and genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others." Legitimate concerns about terrorism and really serious organised crime are behind the legislative provisions and Ministerial directions from the earliest stage. There is no other basis; such as governmental snooping. That does not happen. Further, there is no evidence that any Irish person feels that the inert storage of data with access only on the basis of law excites any fears. An absence of such protection for the population is, instead, a terrifying prospect.

13. According to leading jurisprudents, where the compatibility of a national measure depends closely upon the evaluation of the facts, the interpretation of national law or the interaction between European Union law and national law, "the national court will be much better placed, or indeed the only well-placed, to provide an outcome" since the "factual background may be important, for example in determining whether the requirements of EU legislation are fulfilled or assessing the proportionality of a national penalty." See Professor Takis Tridimas, Bifurcated Justice: The Dual Protection of Judicial Protection in EU Law in Rosas, Livits & Bot, The Court of Justice and the Construction of Europe: Analyses and Perspectives on Sixty Years of Case Law (Asser, 2013) 142, citing Joined Cases C-414 to 416/99 *Davidoff v A&G Imports Ltd* [2001] ECR 1-8691 and Case C-262/99 *Louloudakis v Greece* [2002] ECR 1-5547. Any limitation on a Charter right, here the protection of data, leaving out of consideration for the moment the protection of life and the right not to be violated, is only lawful if it is proportionate. The acquis communautaire establishes a four stage test: (i) does the measure pursue a legitimate goal; (ii) is it suitable to attain that goal; (iii) is it the least restrictive measure available in order to achieve the aim equally well as the measure chosen; (iv) have the competing interests been balanced correctly? See Kellerbauer, Klamert and Tomkins eds, The Eu Treaties and the Charter of Fundamental Rights (OUP, 2019) 2252.

14. That assessment is thus the task of the national courts. There is sufficient evidence now before this Court for a ruling to be made as to whether the decision of the High Court should be reversed or upheld. That is a national task.

Competence in criminal justice

15. The second point is competence in criminal justice, since what is ultimately being sought here by the accused is the exclusion of evidence in a criminal trial context on a charge of murder. In that regard, treaty provisions, derogations and legislative measures must be noted; since these are binding in contrast to the persuasive value of the opinions of jurisprudents. Directive 2002/58/EC of the European Parliament and of the Council of 12 july 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector provides at Article 1.3 that:

> *This Directive shall not apply to activities which fall outside the scope of the treaty establishing the European Community, such as those covered by Titles V and VI of the Treaty on European Union, and in any cast 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.*

16. Even were that not so, proportionality is reflected in Article 15 of the Directive in providing:

> *Member States may adopt legislative measures to restrict the scope of rights and obligations provided for in Article 5, Article 6, Article 8(1), (2), (3) and (4) and Article 9 of this Directive when such restriction constitutes 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 or of unauthorised use of electronic communication system, as referred to in Article 13(1) of Directive 95/46/DC. To this end, Member States may, inter alia, adopt legislative measures providing for the retention of data for a limited period justified on the grounds laid down in this paragraph …*

17. Turning to Directive 2006/24/EC, recital 9 acknowledges that "retention of data has proved to be such a necessary and effective investigative tool of law enforcement in several Member States, and in particular concerning serious matters such as organised crime and terrorism, it is necessary to ensure that retained data are made available to law enforcement authorities for a certain period, subject to the conditions provided for in this Directive." Recital 10 mentions terror attacks and the need to retain data through common measures. Recital 11 also acknowledges this. Those declarations were not made without evidence. In factual terms, that is what this Court is now concerned with.

18. Turning to treaty provisions, Ireland has derogated from Article 82 of the Treaty of Formation of the European Union on judicial cooperation in criminal matters. It is to be noted that minimum rules under Article 82.2 do not apply. Hence, it is not necessary for

Ireland to refer a draft directive to the European Council on the basis that it "would affect fundamental aspects of its criminal justice system". The application of rules undermining criminal investigation and access by victims to justice has that effect. But, that is outside the applicable law. It is worth repeating that this litigation by the accused is to exclude evidence in the criminal justice system of a Member State.

19. With the abolition of the pillar system ushered in by the Lisbon Treaty, the area of freedom, security and justice (covering judicial cooperation) has been integrated into the main body of the Treaties. Article 3 TEU sets out the EU's objectives: "The Union shall offer its citizens an area of freedom, security and justice without internal frontiers, in which the free movement of persons is ensured in conjunction with appropriate measures with respect to external border controls, asylum, immigration and the prevention and combating of crime." Article 4(2)(j) TFEU categorises the area of freedom, security and justice as a shared competence of the EU (Article 4(2)(j) TFEU). Thus, Member States can exercise competence only to the extent that the Union has not exercised, or has decided to cease to exercise, its competence within any such area. The Area of Freedom, Security and Justice is principally dealt with under Title V of the TFEU (Article 67 – 89). Provisions relating to judicial cooperation in criminal matters are found under Chapter 4 of Title V TFEU (Article 82 – 86).

20. Under the Lisbon Treaty, Ireland preserved its ability to opt-out of measures relating to freedom, security and justice. Firstly, under Protocol (No 19) Ireland is not bound by the Schengen agreement but retains the option to participate in some or the entire regime subject to unanimous agreement from participating states. Secondly, Protocol (No 21) sets out that Ireland is not bound by measures adopted under Title V. Furthermore, no international agreement adopted by the EU or decision of the Court of Justice relating to Title V is binding on Ireland. Ireland may decide to participate in a measures adopted under Title V at its own discretion by notifying the Council.

21. In this regard, examples of opt outs and opt ins may assist. Ireland has used Protocol (No. 21) to opt out of a number of Title V measures. These include Framework decision 2009/829/JHA concerning the mutual recognition of supervision measures and alternative provisional detention (European Supervision Order), the European Protection Order (directive 2011/99/EU) and the European Investigation Order (Directive 2014/41/EU), the Roadmap for strengthening procedural rights (and associated measures). Ireland has also opted into a number of Title V measures, including Regulation No 439/2010 establishing a European Asylum Support Office, Directive 2010/64/EU on the right to interpretation and translation in criminal proceedings, Regulation No 1077/2011 establishing a European Agency for the operational management of large scale IT systems in the area of freedom, security and justice (measures concerning EURODAC), Directive 2011/36 EU concerning human trafficking, Directive 2012/13 EU on the right to information in criminal proceedings etc.

22. What is thus clear is that Member States which are part of Title V would have the right to object to measures which could affect the admissibility of evidence. As a matter of logic,

this case is all about excluding vital metadata. Member States within Title V could have made this point to the Commission and sought amendments or clarifications. By being excluded from Title V, Ireland is not part of any legislative obligation for the exclusion of evidence. Further, competence in criminal law is not to be engaged as being within Ireland's treaty obligations through matters related to the internal marked. In the cases of Ireland and Greece, criminal law is specifically excluded from same.

Version Française

L'avis contraire de Monsieur le juge Peter Charleton du 24 février 202

Protection des données

1. L'Irlande a toujours essayé d'assurer un haut niveau de protection des données concernant les télécommunications. Au début, le service postal et de télécommunications a été un monopole d'État. Mais en 1983, l'État a cédé son contrôle sur ce service en créant un nouveau service postal et une nouvelle société de télécommunications. Sous l'article 98 de la loi du service postal et de télécommunications 1983, il est interdit d'intercepter ou de révéler des données concernant les télécommunications. Selon l'article 4 de cette loi, un contrevenant de ce crime est passible d'une peine maximum de 5 ans et d'une grosse amende. Sous la législation moderne, le traitement des données correspond à l'enregistrement et à l'élaboration de données. Selon l'article 98 de la loi 1983, l'interception des données est défendue, sous réserve d'exceptions. L'interception des données est définie comme l'acquisition du contenu ou de la signification de tous les messages télématiques. Cette définition comprend aussi la criminalisation de la révélation de l'existence, du contenu, de la signification et de l'usage de ce type de données. Selon le texte réglementaire 517 de 1997 et plusieurs autres textes réglementaires, des fournisseurs de services doivent garantir la sécurité des données et effacer des données si la conservation de données n'est pas imposée par la loi.

2. L'article 13 de la loi de l'interception des colis postaux et des messages télématiques 1993 ajoute l'article 2A à la loi 1983. Cet article prévoit qu'on ne peut pas être coupable du crime de révélation si on fait la révélation: (a) avec le consentement des parties communicantes; (b) pour la prévention ou la détection du crime ou dans le cadre des procédures pénales ; (c) dans l'intérêt de la sureté de l'État ; (d) quand il y a une ordonnance du tribunal ; (e) quand il y a un ordre de divulgation dans le cadre de procédures civiles ; (f) dans le cadre de ses obligations de travail. Le surintendant principal doit faire une demande par écrit. Si le juge admis en preuve des données, par exemple des données qui indiquent qu'un portable a contacté un autre portable depuis telle ou telle endroit, à telle ou telle heure et pour telle ou telle durée, la légalité de la demande du surintendant principal doit être établi devant la cour par la poursuite à moins que la preuve soit officiellement admise (ce qui est improbable). Donc dans le cadre d'un procès criminel, le Parquet Général est contraint de prouver la légalité de la révélation des données en utilisant l'une des exceptions sous l'article 2A. Cette manière d'obtenir des métadonnées n'est pas contestée. Dans le cadre de droit irlandais, elle reste une mesure législative pour la recherche des criminels et la prévention du crime. La validité de cette mesure législative ne repose pas sur la validité de la directive 2006/24/EC du Parlement européen et du Conseil, du 15 mars 2006, sur la conservation de données générées ou

traitées dans le cadre de la fourniture de services de communications électroniques accessibles au public ou de réseaux publics de communications ou sur la loi des communications (la conservation de données) 2011. La loi 1983, telle que modifiée, prévoit cette manière légale d'accéder aux données. L'interception en temps réel doit être autorisée préalablement par un juge du Tribunal de Grande Instance.

3. Cette affaire traite une poursuite pénale. Chapitre 7, l'article 63 de la loi de la Justice Criminelle (les infractions terroristes) 2005, qui est encore en vigueur, dispose que des données doit être conservées pour une durée de 3 ans. Avant la promulgation de cette loi, selon une direction ordonnée par le Ministre sous l'article 110(1)(b) de la loi 1983, des données doit être conservées en sécurité. Des données deviennent inertes en stockage. D'habitude, des données sont conservées sur un disque dur et sont en cours d'utilisation. Mais des métadonnées, le type des données en question, ne sont pas conservées sur un serveur ou sur un ordinateur, mais sont conservées sur des bobines de bande. Cette forme de stockage est pratique, mais en plus elle assure la sécurité des traitements de telles données. Pour récupérer des métadonnées qui a été conservées pour un an ou dix-huit mois, des bandes doivent être récupérer et passer dans un ordinateur. Ceci donne un niveau de sécurité plus élevé que la sécurité des systèmes actifs qui peuvent être piratés. La législation a réduit la période de stockage pour ce type des données inertes de 5 ans à 2 ans.

Utilité des données dans les affaires criminelles graves

4. Il y a deux exemples qui peuvent montrer l'utilité de la récupération de ce type des bandes et l'utilité d'effectuer une recherche limitée des portables particulier pour les poursuites criminelles. Dans les deux exemples, ce membre de la cour a agi à titre de procureur de la poursuite. En juin 1996, une journaliste distinguée a été tirée par plusieurs balles et a été tuée aux feux de signalisation, près du centre de Dublin, en plein jour. Elle a été suivie par un observateur du Naas au Dublin. A l'époque de l'assassinat, il y avait un gang à Dublin qu'importait des drogues et des armes à feu (y compris des mitraillettes). Il y avait sept membres principaux. Seuls quatre de ces membres avait des condamnations antérieures. Certaines de ces condamnations étaient pour des crimes sérieux mais les policiers n'avaient aucune raison de soupçonner ces quatre membres. Les autres membres n'avaient aucune condamnations antérieures. L'un des membres était au chômage, l'autre était gérant d'une société maritime et le dernier était ancien membre de l'armée. Donc, les policiers n'avaient aucune raison de soupçonner ces trois membres. La journaliste a enquêté sur le gang et sur le chef du gang, au nom du public.

5. Quelques membres du gang a témoigné contre du gang. Ces gens ont été inscrits à un programme de protection des témoins à l'étranger, à cause de la possibilité probable des représailles. Les policiers ont dû faire beaucoup de travail afin d'obtenir la coopération et le témoignage de ces membres. Mais ces gens étaient complices du meurtre et donc, leurs témoignages ont été utilisés avec circonspection par la Cour. L'un des témoins, qui était exportateur de monnaie et qui n'avait pas des condamnations antérieures, a dit aux policiers que le gang lui a ordonné d'aller à Naas, de chercher une voiture rouge et de leur téléphoner. Cette voiture était la voiture de la victime. Des métadonnées ont

corroboré que cet appel a eu lieu et donc a confirmé des témoins. Ces faits et les faits suivants sont empruntés aux arrêts du tribunal pénal spécial et des cours d'appel.

6. Le 15 aout 1998, à Omagh, en Irlande du Nord, des terroristes ont fait exploser une bombe. Vingt-neuf personnes ont été tués, y compris une femme enceinte de jumeaux. L'enquête était méticuleuse et a duré plusieurs mois. Le portable de la personne qui a été accusé du complot, a été analysé. Des métadonnées de ce portable a été récupéré conformément à la législation irlandaise et à la législation britannique. Un portable d'un homme qui a dit qu'il n'a pas participé à l'explosion, a été emprunté. Les autres suspects a dit qu'il a participé. Cet homme, et les autres suspects n'avaient pas des condamnations antérieures et les policiers n'avaient aucune raison de les soupçonner ou de les garder sous surveillance. Sous prétexte de réparer le portable, les autres suspects ont l'emprunté pour le weekend. Des, métadonnées montraient un nombre des appels courts entre les deux portables de Dundalk à Omagh et de Omagh à Dundalk. Comme l'un des portables a été emprunté, il n'avait aucune raison innocente pour ce nombre des appels. Les appels ont été dirigés sur des poteux télégraphiques et le résultat était une série qui était indispensable de déceler et dissuader des crimes sérieux. Le tribunal pénal spécial qui consiste d'un juge du Tribunal de Grande Instance, du Tribunal Correctionnel et du Tribunal de police, a dit que cette preuve a été essentielle. L'extrait suivant est une partie d'un arrêt qui a été annulé en appel pour d'autres motifs:

> *[Le jour de l'attentat de la bombe à Omagh], les nombres des appels entre les deux portables montrent que chaque portable sont allés du compte de Monaghan à Omagh, peu de temps avant l'explosion de la voiture piégée là et ils sont revenus au compte de Monaghan par la suite. Il est très probable que le transport de la voiture piégée à Omagh nécessiterait un véhicule portant la bombe et une voiture qui conduirait en avance. Il est probable qu'il y aurait des contacts téléphones entre les deux véhicules.*

7. Un système où il faudrait obtenir une autorisation préalable, n'aiderait pas à résoudre les meurtres à Omagh et le meurtre de la journaliste. Beaucoup de suspects étaient au-dessus de tout soupçon. En plus, les régions impliquées dans les deux exemples étaient vastes: le premier exemple s'est passé à Dublin, Naas et Cork et le deuxième exemple s'est passé en deux juridiction différentes l'Irlande et l'Irlande du Nord.

Devoir de prouver la légalité de la preuve

8. En droit pénal irlandais, quand le police prend une mesure qui est une intrusion dans les libertés des personnes, dans la maison ou dans les autres droits fondamentaux, il faut fournir une justification légale. Pour être admis comme valable, un juge doit faire l'analyse de cette justification et de la mesure. Ces intrusions ne peuvent qu'être autorisées s'il y a un soupçon raisonnable. Le police et les autres autorités ne peuvent pas porter atteinte aux droits garantis sans un soupçon raisonnable. On ne peut pas accéder aux données concernant les télécommunications sans un soupçon raisonnable et ce soupçon doit être prouvé au procès pénal. Dans l'affaire de *CRH plc contre Competition and Consumer Protection Commission* [2017] IESC 34, le juge a résumé la loi relevant du soupçon raisonnable:

Un soupçon raisonnable est basé sur une raison qui, si elle est contestée, démontrera que la partie qui a fait l'arrestation, qui a émis le mandat ou qui a prolongé la détention, a agi de manière raisonnable; Glanville Williams, "Arrest for Felony at Common Law" [1954] Crim LR 408. Un soupçon raisonnable peut être basé sur l'ouï-dire ou sur un alibi faux; Hussein contre Chong Fook Kam [1970] AC 942: ou l'information d'un dénonciateur fiable; *Lister contre Perryman [1870] LR 4 HL 521, Isaacs contre Brand (1817) 2 Stark 167, The People (DPP) contre Reddan [1995] 3 IR 560. Si le supérieur d'un policier dit un soupçon à le policier ou si un policier dit un soupçon à un autre policier, ces communications peuvent être un soupçon raisonnable si elles suscitent des soupçons raisonnables; The People (DPP) contre McCaffrey [1986] ILRM 687. Si le suspect est acquitté, cela ne veut pas dire que l'arrestation ou la perquisition ne sont pas basés sur un soupçon raisonnable. La Cour européenne des droits de l'homme a dit que « l'existence d'un soupçon raisonnable doit être évaluée au moment de l'émission du mandat »; Robathin contre Austria [2012] ECHR 30457/06 at para. 46.*

Crimes comme des violations des droits de l'homme

9. Le meurtre, le viol et les autres crimes sérieux sont des violations fondamentales des droits de l'homme. L'Article 47 de la Charte des droits fondamentaux de l'Union européenne a dit que « Toute personne dont les droits et libertés garantis par le droit de l'Union ont été violés à droit à un recours effectif devant un tribunal dans le respect des conditions prévues au présent article. » L'expérience confirme la proposition suivante: si on ne conserve pas des données et on n'analyse pas des données dans le cadre d'une enquête criminelle, les crimes sérieux seraient non détectés. Les victimes et les membres suivants de leur famille, seraient privé de leur droit de l'homme d'accès à la justice. Les enquêteurs perdraient un moyen indispensable de déceler des violations des droits de l'homme. La justice doit consister d'une recherche énergique de la vérité et un verdict juste ou la défense des droits de l'homme doivent être basés sur cette recherche. Si on n'utilise pas des preuves indispensables, le résultat serait la déformation du processus judicaire et que la justice ne serait pas rendue. Les criminologues sont d'accord sur le fait que la crainte de détection a un effet dissuasif. L'Irlande a subi le crime organisé et le terrorisme, comme les deux exemples cités ont illustré. En plus, ces exemples montrent qu'une approche modérée de la détection qui protège des droits privés et qui est basé sur un régime juridique, lutte contre ces menaces pour la société.

Raisons pour l'avis contraire

10. Il y a deux raisons pour être en désaccord avec la décision de saisir la Cour de justice de l'Union européenne. Tout d'abord, des cours nationales devraient et peuvent ressourdre la question de la proportionnalité des mesures législative qui empiètent sur des droits fondamentaux. La deuxième raison concerne la compétence en matière de droit pénal de la Cour de justice de l'Union européenne. La question de Kompetenz-kompetenz n'est pas prise à la légère, selon laquelle cette cour prendrait une décision sur sa compétence en matière de droit pénal. Le devoir de coopération sincère nécessite une analyse de l'étendue et des limitations de la compétence nationale et de la compétence de l'Union européenne pour décider qui doit prendre une décision sur la récupération des preuves

pénales. Il ne faut pas saisir la Cour de justice sous l'article 267 du traité sur le fonctionnement de l'Union européenne s'il s'agit d'une question du droit pénal qui doit être résoudre par l'application du critère à quatre volets.

La question de la proportionnalité et de la compétence nationale

11. Dans le cadre de cette affaire, il y avait deux portables qui étaient abandonnés. Des données, qui a été analysé au cours du procès criminel, a prouvé que l'un portable appartient à l'accusé. L'employeur de l'accusé lui a donné l'autre portable. Des armes sont souvent abandonnées à la suite d'un crime. Si la police trouve une arme à feu à long canon, elle peut faire des tirs d'essai pour comparer des striations sur des balles d'essai à la collection des balles de la police. Des marques sur des moulages des balles peuvent associer la douille de balle, qui a été trouvée à la scène du crime, à une arme abandonnée. De la même façon, des empreintes, l'ADN et des fibres qui sont trouvés à la scène du crime peut établir la culpabilité quand ils sont associés aux autres preuves. La collecte des données et l'accès aux données sont les deux faces d'une même pièce. Il n'est pas possible sous la loi européenne que la collecte des données qui est prévoit sous la loi irlandaise, porte atteinte aux droits de l'homme. Si la collecte des données nécessite une autorisation préalable ou un soupçon raisonnable, il ne faudrait pas obtenir autorisation ou avoir un soupçon raisonnable pour accéder aux données. La loi irlandaise prévoit la collecte des données inerte mais l'accès aux données est strictement limité par l'exigence d'un soupçon raisonnable

12. Il incombe aux cours nationaux d'assurer le respecte du droit européen. Sous l'article 8 de la charte, « toute personne a droit à la protection des données à caractère personnel la concernant. » et « ces données doivent être traitées loyalement, à des fins déterminées et sur la base du consentement de la personne concernée ou en vertu d'un autre fondement légitime prévu par la loi ». Ce droit ne doit pas porter atteinte aux droits garantis sous l'article 1, 3 et 6 de la charte parce que l'article 52 prévoit que « toute limitation de l'exercice des droits et libertés reconnus par la présente Charte doit être prévue par la loi et respecter le contenu essentiel desdits droits et libertés. » L'article 98 de la loi 1993, l'article 53 de la loi 2005 et les autres protections du stockage des données, démontrent ce respect. En plus, l'article 52 dit que « Dans le respect du principe de proportionnalité, des limitations ne peuvent être apportées que si elles sont nécessaires et répondent effectivement à des objectifs d'intérêt général reconnus par l'Union ou au besoin de protection des droits et libertés d'autrui. » Ces lois et les directions du ministre sont basées sur des préoccupation légitimes vis-à-vis le terrorisme et le crime organisé. Il n'y a aucune autre base; par exemple, ces lois n'existent pas pour faciliter le gouvernement de fourrer son nez dans les affaires des autres. En plus, il n'y a aucune preuve que les Irlandaises ont peur du stockage inerte des données qui ne sont qu'accéder sur la base du droit. Mais le manque de ce stockage serait effrayé.

13. Selon des juristes, si la compatibilité des mesures nationales avec le droit communautaire dépend de l'appréciation des faits, de l'interprétation du droit national ou de l'interaction entre le droit national et le droit européenne, la cour nationale sera mieux placée pour juger l'affaire parce que les faits peuvent être importants, par exemple, pour décider si

les conditions posées par le droit européenne sont remplies ou pour apprécier la proportionnalité d'une peine nationale. Voir Professeur Takis Tridimas, 'Bifurcated Justice: The Dual Protection of Judicial Protection in EU Law in Rosas, Livits & Bot, The Court of Justice and the Construction of Europe: Analyses and Perspectives on Sixty Years of Case Law' (Asser, 2013) 142, faisant référence aux affaires jointes C-414 à 416/99 Davidoff contre A&G Imports Ltd [2001] ECR 1-8691 et à l'affaire C-262/99 Louloudakis contre Grèce [2002] ECR 1-5547. Une limitation d'un droit garanti par la Charte, dans cette affaire la protection des données, n'est que légale si elle est une limitation proportionnée. Selon l'acquis communautaire, la cour doit résoudre des problèmes de proportionnalité par l'application du critère à quatre volets: (i) est-ce que la mesure a un objectif légitime? (ii) est-ce que la mesure peut atteindre cet objectif? (iii) est-ce que la mesure est la mesure le plus moins restrictif qui peut atteindre l'objectif? (iv) est-ce que les intérêts opposés étaient pondérés correctement? Voir Kellerbauer, Klamert et Tomkins eds, The Eu Treaties and the Charter of Fundamental Rights (OUP, 2019) 2252.

14. Les cours nationales doivent faire cette évaluation. Cette cour a des preuves suffisantes pour décider si la décision du Tribunal de Grande Instance devrait être annulée ou maintenue. Cette décision reste une compétence nationale.

Compétence en matière de droit pénal

15. La deuxième raison pour être en désaccord concerne la compétence en matière de droit pénal de la cour de justice de l'Union européenne. Cette affaire traite l'exclusion des preuves dans le cadre d'un procès pénal pour le meurtre d'une femme. Donc les dispositions du traité, les dérogations et les mesures législatives doivent être pris en compte parce que elles sont obligatoires par contraste avec des opinions des juristes qui n'ont qu'un caractère persuasif. L'article 1.3 de la directive 2002/58/CE du Parlement européen et du Conseil, du 12 juillet 2002, concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (directive vie privée et communications électroniques) prévoit que:

> *La présente directive ne s'applique pas aux activités qui ne relèvent pas du traité instituant la Communauté européenne, telles que celles visées dans les titres V et VI du traité sur l'Union européenne, et, en tout état de cause, aux activités concernant la sécurité publique, la défense, la sûreté de l'État (y compris la prospérité économique de l'État lorsqu'il s'agit d'activités liées à la sûreté de l'État) ou aux activités de l'État dans des domaines relevant du droit pénal.*

16. En plus, la proportionnalité se traduit dans l'article 14 de la directive qui prévoit que:

Les États membres peuvent adopter des mesures législatives visant à limiter la portée des droits et des obligations prévus aux articles 5 et 6, à l'article 8, paragraphes 1, 2, 3 et 4, et à l'article 9 de la présente directive lorsqu'une telle limitation constitue une mesure nécessaire, appropriée et proportionnée, au sein d'une société démocratique, pour sauvegarder la sécurité nationale - c'est-à-dire la sûreté de l'État - la défense et la sécurité publique, ou assurer la prévention, la recherche, la détection et la poursuite d'infractions pénales ou d'utilisations non autorisées du système de communications

électroniques, comme le prévoit l'article 13, paragraphe 1, de la directive 95/46/CE. À cette fin, les États membres peuvent, entre autres, adopter des mesures législatives prévoyant la conservation de données pendant une durée limitée lorsque cela est justifié par un des motifs énoncés dans le présent paragraphe …

17. Dans le cadre de la directive 2006/24/EC, selon paragraphe 9 du préambule, « la conservation de données s'est révélée être un outil d'investigation nécessaire et efficace pour les enquêtes menées par les services répressifs dans plusieurs États membres et, en particulier, relativement aux affaires graves telles que celles liées à la criminalité organisée et au terrorisme, il convient de veiller à ce que les données conservées soient accessibles aux services répressifs pendant un certain délai, dans les conditions prévues par la présente directive. » Le paragraphe 10 du préambule fait référence aux attentats terroristes et à la nécessité d'adopter des mesures communes relatives à la conservation de données concernant les télécommunications. Cette disposition n'est pas sans fondement et ils portent sur les faits de cet affaire.

18. En ce qui concerne des dispositions des Traités, l'Irlande a dérogé à l'Article 82 du traité sur le fonctionnement de l'Union européenne sur la coopération judiciaire en matière pénale dans l'Union. On doit noter que les règles minimales de l'Article 82.2 n'applique pas en Irlande. Donc, s'il y a un projet de directive qui « porterait atteinte aux aspects fondamentaux de son système de justice pénale, » l'Irlande ne doit pas saisir le Conseil européenne. L'application des règles qui sape les enquêtes criminelles et l'accès de justice des victimes, a cet effet. Encore une fois, cet affaire s'agit de l'exclusion de preuves dans le cadre d'un procès pénal d'un État Membre.

19. Le traité de Lisbonne 2009 n'a pas retenu la structure en piliers et donc l'espace de liberté, de sécurité et de justice (qui comprend la coopération judiciaire) a été intégré dans les traités. Selo l'article 3 du traité sur l'union européenne, « L'Union offre à ses citoyens un espace de liberté, de sécurité et de justice sans frontières intérieures, au sein duquel est assurée la libre circulation des personnes, en liaison avec des mesures appropriées en matière de contrôle des frontières extérieures, d'asile, d'immigration ainsi que de prévention de la criminalité et de lutte contre ce phénomène. ». En plus, l'article 4(2)(j) du traité sur le fonctionnement de l'Union européenne prévoit que l'espace de liberté, de sécurité et de justice est une compétence partagée. Donc, les Etats membres ne peuvent qu'exercer leur compétence dans la mesure où l'Union n'a pas exercé la sienne ou a décidé de cesser de l'exercer. L'espace de liberté, de sécurité et de justice est traité au titre V du traité sur le fonctionnement de l'Union européenne (de l'article 67 à l'article 89) et la coopération judiciaire est traitée au chapitre 4 du titre V (de l'article 82 à l'article 86).

20. Sous le traité de Lisbonne, l'Irlande peut choisir de ne pas adhérer aux mesures concernant l'espace de liberté, de sécurité et de justice. Tout d'abord, le protocole (no 19) prévoit que l'Irlande ne participe pas à toutes les dispositions de l'acquis de Schengen mais elle peut à tout moment demander de participer à tout ou partie des dispositions de l'acquis de Schengen si tous les autre États membres qui participent à l'acquis Schengen,

sont en accord. Deuxièmement, le protocole (no 21) prévoit que l'Irlande ne participe pas à l'adoption par le Conseil des mesures proposées relevant du titre V du traité sur le fonctionnement de l'Union européenne. En plus, l'Irlande ne participe pas à aucune disposition de tout accord international conclu par l'Union en application de ce titre et aucune décision de la Cour de justice de l'Union européenne interprétant ces dispositions ou mesures. L'Irlande peut décider de participer à l'adoption et à l'application d'une mesure proposée relevant du titre V mais le Conseil doit être en accord.

21. L'Irlande a participé aux mesures relevant du titre V et a choisi ne pas adhérer aux mesures relevant du titre V. L'Irlande n'a pas participé à la décision-cadre 2009/829/JAI du Conseil qui concerne le principe de reconnaissance mutuelle aux décisions relatives à des mesures de contrôle en tant qu'alternative à la détention provisoire, au directive 2011/99/UE relative à la décision de protection européenne, au directive 2014/41/UE concernant la décision d'enquête européenne en matière pénal et à la résolution du conseil relative à la feuille de route visant à renforcer les droits procéduraux des suspects ou des personnes poursuivies dans le cadre des procédures pénales. D'autre part, l'Irlande a participé au règlement 439/2010 portant création d'un bureau européen d'appui en matière d'asile, au directive 2010/64/UE relative au droit à l'interprétation et à la traduction dans le cadre des procédures pénales, au règlement 1077/2001 portant création d'une agence européenne pour la gestion opérationnelle des systèmes d'information à grande échelle au sein de l'espace de liberté, de sécurité et de justice, au directive 2011/36/UE concernant la prévention de la traite des êtres humains et au directive 2012/13/UE relative au droit à l'information dans le cadre des procédures pénales.

22. Il est clair que les États Membres qui participe au titre V, a le droit de ne participer pas aux mesures relevant de l'admissibilité des preuves. Cet affaire s'agit de la question de l'admissibilité des métadonnées. Les États Membres qui participent au titre V auraient pu proposer des amendements ou obtenir des éclaircissements de la Commission. En raison du titre V, l'Irlande ne doit pas participe aux mesures relevant de l'admissibilité des preuves. En plus, la compétence en matière du droit pénal ne s'engage pas en raison de d'être partie des obligations irlandaises relatant au marché intérieur. En ce qui concerne l'Irlande et la république hellénique, elles se sont exclus.