THE HIGH COURT

JUDICIAL REVIEW

[2024] IEHC 37

Record No. 2021/707/JR

BETWEEN

RAJA NASEEB

PLAINTIFF

AND

THE DIRECTOR OF PUBLIC PROSECUTIONS

RESPONDENT

JUDGMENT of Mr. Justice Nolan delivered the 7th of Febuary, 2024

Introduction

1. This is an application for judicial review brought by the applicant under Order 84 of the Rules of the Superior Courts for an order of prohibition by way of judicial review restraining the respondent, her servants or agents, from prosecuting the applicant in regard to three counts of engaging in converting, transferring, handling, acquiring, possessing or using property that are the proceeds of criminal conduct contrary to s. 7 (1) (A) (ii), 7 (1) (B) and 7 (3) of the Criminal Justice (Money Laundering and Terrorist Financing) Act 2010.

2. In essence, the respondent alleges that the applicant on various dates between the 13th of November 2017 and the 22nd of November 2017 within the State, knowingly or believing (or being reckless as to whether) money credited to the applicant's account by various banks were the proceeds of crime and that he dealt with the monies in the account in the knowledge that they were the proceeds of crime or alternatively reckless as to whether the proceeds of crime, sending the money on to third parties.

3. The kernel of the applicant's case is neatly summarised by way of the third declaration which he seeks by way of judicial review, namely that there is a real risk that he will not receive a fair trial by reason of the failure of An Garda Síochána to retrieve for inspection the Internet Protocol addresses ("the IP addresses") from which each money transfer was performed from each bank account connected to the applicant and associated records to establish which physical address those IP addresses / records relate to.

4. The respondent alleges that any alleged failure are matters which can be dealt with by the trial judge by way of direction to the jury and that has been delay in bringing this application.

Factual Background

5. At all material times, the applicant held bank accounts with three financial institutions namely KBC Bank, account number 11629137 in the name of "Raja Umer Naseeb", PTSB account number 25029380 in the name of "Raja Umer Naseeb", and An Post account number 10525523 in the name of "Raja Umer Naseeb".

6. At all material times he resided at 8, Dromard, Cashel Road, Clonmel, Co. Tipperary.

7. Many miles away, Felix O'Hare and Company Builders started working at Ardee Community School at the behest of Louth Meath Education and Training Board ("LMETB")

in January of 2017. It was agreed that they would be paid by an electronic fund transfer, known as an EFT, for the duration of the project.

8. On the 7th of November 2017, the finance officer of LMETB received a telephone call from a person claiming to be an employee of the construction company requesting that the bank account details which had previously been furnished were to be changed for the next payment. Thereafter, emails were sent and received by LMETB, from somebody with an email address at amandamoore@felixohare.com on the 7th and 8th of November 2017. Initially it was requested that all future transactions would be made payable to a HSBC Bank account registered in Co. Down. However, when advised that that was not possible, the bank details of an Ulster Bank account were furnished and on the 10th of November 2017, €247,896.54 was transferred by LMETB into that account.

9. Thereafter, those funds were transferred to various other accounts including the three accounts held by the applicant, creating what the applicant describes as a *"complex web of financial transactions".*

10. It will not come as a surprise that it transpired "Amanda Moore" was not employed by Felix O'Hare and that the email address had nothing to do with the construction company, nor indeed did the construction company have any connection with the Ulster Bank account furnished.

11. Thereafter, a complaint was made to An Garda Síochána and an investigation commenced. On foot of that investigation applications were made to the District Court on the 20th of December 2017 and the 2nd of January 2020 permitting the uplifting of account statements, documentation, and details on various financial institutions together with IP address details and CCTV footage.

12. On the 27th of February 2018 a search warrant was obtained permitting An Garda Síochána to carry out a search at his home in Clonmel. The next day, on the 28th of February

2018, the house was searched, and a number of items were seized including a letter from KBC Bank, another letter from PTSB and a receipt from An Post together with a black Apple iPad. Thereafter, the applicant was arrested, detained and interviewed.

13. Over the course of two interviews the applicant stated he knew nothing of the KBC account or the An Post account registered in his name, or of any of the alleged transactions associated with the accounts. He did, however, accept that he had set up the Permanent TSB account but stated that he had stopped using it some months previously because he was unable to gain access. He denied and still denies any knowledge of the relevant transfers.

14. On the 8th of February 2020, the plaintiff was charged with the offences set out above and returned for trial to Clonmel Circuit Court. Thereafter, the matter was listed for the first time on the 29th of September 2020. The applicant sought disclosure from the respondent on the 5th of November 2020 including the IP addresses from which each money transfer was allegedly performed from each bank account connected with the applicant and the associated records to establish which physical address those IP records related to.

The Engagement with An Garda Síochána in relation to the IP Addresses

15. In or around this time, legal aid was extended to cover the preparation of an IT expert report. In response to the disclosure request, the respondents stated that they had not obtained the IP addresses in relation to the transfers by letter dated 28th of May 2021.

16. On the 24th of January 2022, however, the respondent advised that they did have an IP address relating to the PTSB account but didn't realise that they had it because it had been saved under an incorrect title. Unfortunately, they did not obtain the IP addresses in relation to the KBC Bank account nor the An Post bank account. The respondent asserted that since the request for the data was served two years after the allegation occurred, it wasn't available.

17. The IP address which was obtained in relation to the PTSB bank accounts were attributed to locations in the United States and the Netherlands. Mr. Power SC, for the applicant, confirms that the applicant is not proceeding with his case in relation to the PTSB bank account since the IP addresses were furnished.

The District Court (Criminal Justice) Act, 1994 s. 63 application

18. As noted above in the month of December 2017, An Garda Síochána made an application to the District Court for documentation pertaining to the bank accounts and in particular the KBC bank account 11629137. The documentation included the account opening documentation, identification papers produced to support the account opening application, the statements of account for the period 1st of January 2017 up to December 2017, and crucially all documentation relating to all transactions occurring on this account for a period of the 1st of January 2017 to current date or account closure date including IP addresses for transactions conducted online. Finally, all CCTV footage relating to the transactions were requested.

19. Thereafter, the District Court made an order pursuant to Section 63 (3) (b) of the District Court (Criminal Justice) Act 1994. That application was grounded on information furnished by Det. Gda. O'Meara. The reason given was that the documentation including the IP addresses would be of substantial value (whether itself or together with other material) for the purposes of the investigation. He reiterated that the documents were integral to the proper investigation of the matter. A similar application was made by other members of An Garda Síochána to the same District Judge on the same day relating to the other bank accounts.

20. The District Court order noted that there were reasonable grounds for believing that the material should be produced or that access to it should be given, having regard to the benefit likely to accrue to the investigation and other relevant circumstances.

The IT Consultant's Report

21. Mr. Ross Donnelly, forensic scientist, of Keith Borer Consultants, Durham, England, was engaged on behalf of the applicant. In various letters and indeed in his witness statement, Mr. Donnelly emphasises the importance of an IP address. It is a number used to uniquely identify a network attached device, such as a computer or router. An external IP address is globally unique and is required for each device to be directly connected to the internet, commonly by way of a router. Any device on an internal network using that router to access the internet would be externally identifiable only by the IP address of the router.

22. An external IP address is a unique identifier on the internet and is assigned by the internet service provider ("ISP") to each connection. In his submissions, Mr. Power describes the IP address as being *"a forensic fingerprint".*

23. He makes the point that transferring funds into an account does not require the permission or knowledge of a recipient or account holder. In this case, the activity of relevance relates to outgoing transfers and withdrawals from the accounts, demonstrating knowledge of the funds within the account. Anyone with access to the relevant bank accounts could be responsible for the onward transfer of the funds. The crucial point being that any IP address logs which are generally retained by the bank, could offer a cross reference with transactions, and establish the IP address and subsequently attempt to resolve to a physical location that a transaction was performed from.

24. In the absence of such logs, it is not possible to ascertain from whom or from where the bank accounts of interest were accessed.

25. It is in these circumstances, of what is described as "*the loss of the IP addresses*" that this application is brought.

The Applicant's Submissions

26. Mr. Power states that the missing IP address gives rise to a real possibility that the applicant would be unable to advance a point which would be material in his defence. The Gardaí failed in their investigative role to seek and preserve crucial information, which will have a crucial bearing on the applicant's defence. Had the IP address data in question been obtained and kept, it could have identified the exact time and location from where the EFTs were conducted. It could not necessarily identify who undertook the EFTs but it would allow the applicant to adduce evidence that he was elsewhere at the relevant time. Thus, the applicant is being deprived of this significant line of defence.

27. Mr. Power goes somewhat further, stating that the Gardaí didn't even know that they had got the IP address in the case of the PTSB account.

28. The key to this case, however, is the fact that Section 11 of the Criminal Justice (Money Laundering and Terrorist Financing) Act 2010 imposes a presumption on an accused person which shifts the burden of proof. To be fair to Mr. Power, he resiles from one assertion in his written submission, namely that the onus upon the applicant is to prove "*beyond a reasonable doubt*" that he did not know the money was in his bank account. That does not seem to be the position. Nonetheless, the applicant needs to be able to interrogate the evidence and without the evidence, he is at a significant disadvantage. Mr. Power says that Section 11 is not something which is hypothetical. The Gardaí made a mistake. In particular, the Gardaí were themselves clearly aware of the importance of the IP addresses since they swore information before the District Court in relation to the three bank accounts.

29. Further, he makes the point that the Gardaí didn't even know what they had, in that the IP address of the PSTB account only came to the fore late in the day.

The Submissions of the Respondent

30. Mr. McGuinn SC, for the respondent, invites the court to consider three issues. Firstly, the exceptional jurisdiction of the court in Section 11 type cases, secondly to engage with the facts, and thirdly the role of the trial judge in these matters.

31. In relation to the first of these, namely the exceptional jurisdiction, he believes there is a fundamental misunderstanding in relation to Section 11. So long as the accused can put forward an explanation as to how the money came into his account, then the onus of proof shifts to the prosecution. Thereafter, he has referred me to a number of cases which I will set out below in relation to the jurisdiction to prevent the trial proceeding.

32. In relation to the facts, he disputes the suggestion that the IP address is a digital fingerprint. Unlike a fingerprint, it does not identify who was using the computer. Further, the use of technology in the form of VPNs, which is a virtual private network which encrypts one's internet traffic and protects one's online identity can disguise the true address. In fact, the IP address often can tell one very little information. He argues that the failure to have an IP address could indeed assist the defence. It can only assist the prosecution if the accused is right beside the device being used. Therefore, the failure to not have an IP address is in no way fatal to the defence of the accused.

33. He argues that the fact that there is no IP address means that the defence now have a new line of defence to raise at the trial. The jury will have to consider this argument that somebody else may have taken control of his account. But he points out that the flow of money into the applicant's account is highly questionable.

34. In this regard, he sets out what the prosecution says actually took place. The applicant admitted he opened the PTSB account but asserted that he did not have access to it for months. He claimed to know nothing about the KBC account, but he was living with somebody who might have used his details. He named that person. Further, he alleged that

the email account which opened the KBC account was not his, nor had he ever opened or used an An Post account.

35. When contents of his iPad were put to him, he was unable to explain why there was a KBC App on the device or photographs used to open the KBC account as well as details of the PTSB account which included the transfer of a significant sum from a third party on the 17th of November 2017.

36. The respondent says the evidence against the applicant is not based on the issue of the IP address data. There is relevant evidence relating to the opening of bank accounts, documentation bearing his details and identity, and the paperwork in relation to all three accounts which were found in his bedroom.

37. Further, there is CCTV footage of withdrawals from his PTSB account during a time when he alleged that he did not have control of his account, and more particularly footage of him making withdrawals on the 16th and 17th of November 2017 in Clonmel, after the stolen funds were lodged into his account on the 13th and 14th of November 2017.

38. It is the case of the respondent that at a minimum, the applicant allowed his bank accounts to be used for money laundering purposes and then allowed his online passwords and codes to transfer his funds to other bank accounts.

39. Of the €246,896.54 stolen, approximately €100,000 which are the proceeds of criminal conduct, went through the three bank accounts held in the name of the applicant.

40. The final issue relates to the role of the trial judge. Mr. McGuinn says that this is a classic example of a type of matter which the trial judge should be allowed to give an appropriate direction to the jury about. Indeed, the written submissions make multiple references to the role of the trial judge in these matters.

Section 11 of the Criminal Justice (Money Laundering and Terrorist Financing) Act of 2010

41. Under the heading of "*Presumptions and other matters*", s. 11 (2) of the 2010 Act says as follows: -

> *"(2) In proceedings for an offence under section 7, 8 or 9, where an accused has engaged, or attempted to engage, in specified conduct (defined in s. 11 (1)) in relation to property that is the proceeds of criminal conduct, in circumstances in which it is reasonable to conclude that the accused—*
>
> *(a) knew or believed the property was the proceeds of criminal conduct, or*
>
> *(b) was reckless as to whether or not the property was the proceeds of criminal conduct,*
>
> *the accused is presumed to have so known or believed, or been so reckless, unless the court or jury, as the case may be, is satisfied, having regard to the whole of the evidence, that there is a reasonable doubt that the accused so knew or believed or was so reckless".*

42. The key issue in this case is the effect of the reversal of burden of proof.

43. It seems to me that the issue of the reversal of the burden of proof is not new in Irish criminal law. Indeed, in the case of the *DPP v Forsey* [2016] IECA 233, Ryan P. said that the question of the reverse burden of proof had been the subject of a great deal of discussion in judicial and academic circles in recent years and was the principal issue in that appeal. The question in that case is whether Section 4 of the Prevention of Corruption Act, 1906 as amended, imposed a legal or an evidential burden of proof on the accused. The court concluded that it imposed a legal burden on the accused in a case of corruption where the necessary statutory elements had been proved beyond reasonable doubt. The provision was held not to be unconstitutional.

44. In this case, Mr. McGinn has stated that if the applicant gives an explanation, as to how the money came to be in his accounts then in those circumstances the onus on proof shifts back to the prosecution.

The Duty to Seek and Preserve Evidence.

45. Having heard the submissions of both parties it seems to me that there is little between them in relation to the law. In *Braddish v The DPP* [2002] ILRM 151 the Supreme Court held that it was a well-established principle that evidence relevant to the guilt or innocence of an accused must, as far as is necessary and practicable, be kept until the trial concluded. In that case there was a dispute as to whether still photographs taken from a video which had been lost, could be introduced into evidence. Judge Haugh (as he then was) excluded the stills on the basis that it would be unfair to produce them when the video from which they had been taken was not available to the defence. That was the issue which came before the Supreme Court. The court found that it was the duty of the Gardaí to seek out and preserve, so far as is fair and reasonable, all evidence relating to the guilt or innocence of the accused, regardless of whether the Gardaí would seek to rely on that evidence during the trial and regardless of its usefulness to the prosecution or the accused's case.

46. That decision was reiterated in the case of *Dunne v The DPP* [2002] 2 ILRM and more recently in the case of *The People (at the Suit of the Director of Public Prosecutions) v S.Q.* [2003] IESC 8, which highlighted the duty on the prosecution to seek out and preserve evidence. In that case Baker J. said:

> *"22. The duty to investigate crime has at its corelative the duty to seek out and preserve evidence, and to disclose it to a defendant. Thus, the duty of the prosecution authorities, in practice one that rests on the gardaí, to seek out and disclose evidence is central to, and supports, fair trial rights and goes some way to redressing the*

imbalance between prosecution and defence in the light of the powers of the gardaí to investigate and collect evidence."

However, that duty must be seen in the light of the Supreme Court decision of *Savage v DPP* [2009] 1 IR 185, where Denham J. (as she then was) set out the relevant principles.

47. I do not intend to repeat them but suffice to say that top of the list is that each case should be determined on its own particular circumstances. Further, the court has a duty to protect due process. The duty to preserve and disclose cannot be precisely defined as it is dependent upon all the circumstances of each individual case. The duty should be interpreted in a practical manner on the facts of the case.

48. Dealing with the issue of missing evidence there are a number of leading decisions as to how the court should assess the effect of missing evidence. They are quoted at length in the submissions of the respondent. One of these principles is that the applicant must show by reference to the case to be made by the prosecution, in effect the book of evidence, how the allegedly missing evidence will affect the fairness of his trial. The essential question is whether there is a real risk of an unfair trial (see *Dunne v Director of Public Prosecutions* [2002] 2 IR 305, *Bowes v Director of Public Prosecutions* [2003] 2 1 IR 25, *McFarlane v Director of Public Prosecutions* [2006] IESC 11 and *Byrne v Director of Public Prosecutions* [2011] 1 IR 346).

49. In *Byrne* O'Donnell J. (as he then was) said as follows: -

"*In my view, having considered the decided cases, the position has now been reached where it can be said that, other than perhaps the very straightforward type of case as in Branddish v DPP, it would now require something exceptional to persuade a court to prohibit a trial."*

Warming to his theme he said as follows: -

"The constitutional right, the infringement of which is alleged to ground an applicant's entitlement to prohibit a trial, is the right to fair trial on a criminal charge guaranteed by Articles 38 and 34 of the Constitution. The manner in which the Constitution contemplates that a fair trial is normally guaranteed is through the trial and, if necessary, appeal processes of the courts established under the Constitution. The primary onus of ensuring that that right is vindicated lies on the court of trial, which will itself be a court established under the constitution and obliged to administer justice pursuant to Article 34. It is, in my view, therefore entirely consistent with the constitutional order to observe that it will only be in exceptional cases that superior courts should intervene and prohibit a trial, particularly on the basis that evidence is sought to be adduced (in the case of video stills) or is not available (in the case of CCTV evidence itself).

Delay

50. The respondent makes a case in relation to delay in the circumstances where there was no disclosure complaint made to the trial court on the 3rd of November 2020 or any reservation expressed by the applicant in relation to the fixing of a trial date on the 2nd of November 2021. Indeed, the request for disclosure only came two days after the first trial date of the 3rd of November 2020. The application for judicial review was made on the 26th of July 2021. This argument is relevant given the fact that the IP information was sought in relation to the An Post bank account very late in the day.

Decision

51. While the use of computers in day-to-day life is ubiquitous, what happens behind the screens is often seen as a great mystery. I have little doubt that ten years ago, or even less,

the concept of an IP address would be unknown to the vast majority of the general public. However, precisely how important it is in the context of this case seems to me to be overstated. Initially the applicant believed that all IP addresses had been lost or not retrieved by An Garda Síochána. It transpired that in fact An Garda Síochána had obtained the IP addresses used in the PTSB account. However, as Mr. Power said, *"they didn't know what they didn't know"*. But what was disclosed seems to raise more questions than answers, since the IP addresses were located in America and in the Netherlands. Precisely how this assists the applicant is unclear to me.

52. Further, as the respondent has set out the use of a VPN or other devices to hide the IP address is commonplace. Anybody who is in the company of teenage children will no doubt be aware of their proclivity to use VPN's and other devices to hide the IP address order to stream online video material, which is not readily available in this jurisdiction.

53. Given that the applicant himself has described the fraud in this case as a *"complex web of financial transactions"*, it is highly unlikely that the thieves would leave their calling card in the form of an easily identifiable IP address.

54. While I readily accept the duty placed upon An Garda Síochána is to seek and preserve all evidence, particularly in circumstances where there is a shifting of the burden of proof, pursuant to Section 11, it does not seem to me that the missing evidence is so significant so as to give rise to a risk that the applicant will not receive a fair trial. I do not believe that the unavailability of the IP address will deprive the applicant to advance a full defence. Indeed, the very fact that the IP address is not available, seems to me to potentially give the applicant a further line of defence. With the appropriate warning to the jury from the trial judge, any potential risk of injustice should be dealt with.

55. In the circumstances I dismiss the application.

56. I will hear submissions in relation to costs.