What to do when dawn raids happen

Davinia Brennan, Associate, A&L Goodbody, ***provides an in depth analysis of a recent decision of the Irish High Court on the scope of search warrants — and provides ten tips for organisations to be cognizant of during dawn raid investigations***

Being supervised by a labyrinth of regulators, organisations in Ireland face a very real and present risk of a regulatory investigation or dawn raid. Although regulators have wide-reaching search and seizure powers (including the ability to conduct unannounced inspections), organisations benefit from certain safeguards under privacy laws. In addition, the European Court of Human Rights ('ECtHR') exercises a close scrutiny over whether such safeguards are applied in a practical and effective, rather than a theoretical and illusory, manner. Thus the challenge for organisations is to understand how to deal with unannounced inspections and co-operate with investigators, whilst protecting their privacy rights.

In the recent case of *CRH PLC, Irish Cement Ltd and Seamus Lynch v The Competition and Consumer Protection Commission* ('CCPC') (5th April 2016), the Irish High Court determined that the seizure by the CCPC of the entire contents of a professional email account of an employee, containing documents unrelated to the investigation as well as personal emails, was unlawful.

Although the decision relates to the search and seizure regime under the Competition and Consumer Protection Act 2014 ('the 2014 Act'), the case serves as a warning to other regulators to ensure that they respect organisations' privacy rights when exercising their search and seizure powers during dawn raids.

The right to privacy — background

Although the Irish Constitution does not expressly recognise a general right to privacy, such a right has been recognised as being implied from Article 40.3 of the Constitution since the date of the decision of the Supreme Court more than four decades ago in *McGee v Attorney* General [1974] I.R. 284.

However, the right is not an unqualified right, and may be limited or restricted in the interests of the common good, public order and morality.

In *Digital Rights Ireland Ltd v Minister for Communications &* Ors [2010] 3 IR 251, the High Court confirmed that the right to privacy extends to companies as legal entities, separate and distinct from their members as natural persons.

Article 8(1) of the European Convention on Human Rights ('ECHR') guarantees the right to respect for private and family life, for the home and for correspondence. Again, this right is not absolute. Article 8(2) of the ECHR provides that: *"There shall be no interference by a public authority with the exercise of this right except such as [1] in accordance with the law and [2] is necessary in a democratic society [a] in the interests of national security, public safety or the economic well-being of the country, [b] for the prevention of disorder or crime, [c] for the protection of health or morals, or [d] for the protection of the rights and freedoms of others".*

The European Convention on Human Rights Act 2003 gives effect to the ECHR in Irish law. It requires the courts to interpret Irish law insofar as possible in line with the ECHR, and requires public bodies (such as regulators) to perform their functions in a manner compatible with the ECHR.

In *Sociétés Colas Est v France* (16th April 2002), the ECtHR confirmed that in certain circumstances, the rights guaranteed by Article 8 of the ECHR may be construed as including the right to respect for a company's registered office, branches or other premises.

Articles 7 of the EU Charter of Fundamental Rights of the EU ('the Charter') provides for the right to respect for private and family life, and Article 8 provides for protection of personal data. Article 51 of the Charter provides that the provisions of the Charter are addressed to Member States only when they are implementing EU law.

The facts of the case

In May 2015, authorised officers of the CCPC, acting pursuant to a search warrant issued under section 37 of the 2014 Act, carried out a dawn raid of business premises of a party under investigation for anti-competitive practices in the bagged cement sector.

In the course of that raid, the officers obtained a copy of the entirety of the email box of a (now former) senior executive, who is currently the Managing Director of another entity within the

group to which the party under investigation belongs.

Some of the emails and attachments in the email box were almost certainly not caught by the terms of the warrant, as they included documents relating to other companies within the group as well as personal emails. This was not information that 'may be required in relation to a matter under investigation' as required by section 37 of the 2014 Act. The central issue before the court was what was to be done about those emails which it was claimed that the CCPC did not lawfully have in its possession.

The CCPC contended that it had the right to go through all the material it had seized to determine what material it was entitled to take away. The plaintiffs, on the other hand, claimed that for the CCPC to review the material which it was not entitled to take away contravened the right to privacy, be it in the form arising under the ECHR or the Constitution, or both.

Reliefs sought

At trial, the plaintiffs sought the following:

- a declaration that the CCPC had acted 'ultra vires' (beyond its powers), contrary to the 2014 Act, and outside the scope of its search warrant;
- a declaration that the CCPC had acted in breach of the Data Protection Acts 1988 and 2003 ('the DPAs');
- a declaration that the CCPC had acted in breach of Articles 7 and 8 of the Charter;
- a declaration that the CCPC had acted in breach of the plaintiffs' right to privacy under Art.40.3 of the Constitution;
- a declaration that the CCPC had acted in contravention of Article 8 of the ECHR; and
- an injunction restraining the CCPC from accessing, reviewing or making any use of the documents seized, which do not relate to an activity in connection with the business of supplying or distributing goods or providing a service at the premises of the business.

The decision

The High Court said that the bulk seizure was outside the scope of the search warrant issued under section 37 of the 2014 Act, and that examination by the CCPC of the bulk data would constitute a breach of the right to privacy under Article 40.3 of the Irish Constitution and Article 8 of the ECHR.

It therefore granted a declaration that certain materials seized by the CCPC during its dawn raid were not covered by the terms of the applicable search warrant and were done without authorisation under section 37 of the 2014 Act.

The Court noted that there is nothing in the 2014 Act to indicate what should be done regarding material which has been seized but ought not to have been seized, as the material does not relate to a matter under investigation. It granted an injunction restraining the CCPC from accessing, reviewing or making any use of the seized material pending any agreement that might be reached between the parties on how to sift out the relevant and irrelevant material.

The Court also noted the existence of a perfectly operable process in section 33 of the 2014 Act whereby material that is seized and which is claimed to be legally privileged is vetted impartially with a view to determining whether that privilege has been correctly claimed, and thus whether the State should view that material. The Court found that there was no reason why such a process could not have been voluntarily agreed between the CCPC and the plaintiffs in this case.

The Court refused to grant declarations that the CCPC had breached the DPAs or Articles 7 and 8 of the Charter. It also refused to grant a declaration that the CCPC had contravened Article 40.3 of the Constitution or Article 8 of the ECHR, but it considered that if the CCPC was to proceed as it intended (i.e. to go through all the material that it had taken away and determine what is the material that it was entitled to take away), that those provisions of the Constitution and the ECHR would be breached.

Addressing each legislation in turn — why did the Court find the CCPC's dawn raid was not contrary to the DPAs, Charter, Constitution or ECHR?

The DPAs

The Court noted that section 8 of the DPAs contains exemptions regarding the processing of personal data which is required for the purpose of investigating offences, or which is required under any enactment or by order of the court. It found that there was a very wide breadth of information — including personal data — that the CCPC was entitled to take away with it after the dawn raid, by virtue of the combined effect of its search warrant and section 37 of the 2014 Act.

One of the judges noted that, to the extent that the CCPC was not entitled to any personal data being sought, it was open to the party under investigation in these proceedings to refuse to release that data to the CCPC. Insofar as that party elected to release data to which the CCPC was not entitled, it is liable as data controller for its breach of the DPAs, not the CCPC. However, once the data were disclosed to the CCPC, it had a responsibility to process the data in accordance with the DPAs.

The Charter

Barrett J. found that Article 51 of the Charter provides that the Charter's provisions are addressed to Member States only when they are implementing EU law. In the Court's view, section 37 of the 2014 Act (under which the search warrant was issued) was not a statutory provision implementing EU law in the context of this case, because the CCPC was not acting to implement EU law (although there are circumstances when it could be).

Therefore no argument as to contravention of the Charter could succeed in these proceedings.

(Continued on page 6)

(Continued from page 5)

The Constitution

The Court held that each of the plaintiffs enjoys a constitutional right to privacy which can only be interfered with in a justifiable and proportionate manner.

However the Court was not prepared to grant a declaration that the CCPC had acted in breach of the plaintiffs' right to privacy under Article 40.3 of the Constitution.

The real difficulty arose with the CCPC determining what was to happen in respect of the materials seized (other than legally privileged materials) which did not relate to the matter under investigation. Barrett J. stated that if the CCPC was to trawl through the material and determine what it was entitled to take away, "it would quite literally be engaging in an entirely unwarranted — not to mention egregious — transgression of the right to privacy of the plaintiffs in these proceedings". The Court concluded that such an examination would contravene Article 40.3 of the Constitution.

This aspect of the ruling means that the appointment of an impartial third party to assess the relevance of material seized by the CCPC (particularly electronic data) during a dawn raid is likely to become a part of Irish competition law enforcement actions going forward.

The ECHR

The parties accepted that the dawn raid of the business premises and the copying of the records could constitute an interference by a public authority with the private life of one or more of the plaintiffs, contrary to Article 8(1) of the ECHR. So the sole issue for the court was whether such interference occurred in accordance with law, and was necessary in a democratic society (i.e. proportionate to the legitimate aim pursued) pursuant to Article 8(2).

The Court considered European case-law showing how dawn raids of businesses can violate the right to privacy guaranteed by Article 8 of the ECHR. For example, in *Niemetz v Germany* (1993) 16 EHRR 97, the ECtHR held that a search of the plaintiff lawyer's office amounted to a breach of Article 8 because the warrant was drawn in such broad terms that it ordered a search for and seizure of documents without any limitation, and was disproportionate in the circumstances.

Also in *Robathin v Austria* (3rd July 2012) which concerned a search and seizure of electronic data at a lawyer's office, the ECtHR condemned 'general searches' of electronic documents which are not reasonably limited in their scope, and found the search warrant to be couched in very broad terms which went beyond what was necessary to achieve the legitimate aim. Further, in *Vinci Construction v France* (2nd April 2015), the ECtHR found France to be in violation of the ECHR in respect of inspections carried out at business premises, as the seizures included the entirety of certain employees' professional email accounts, as well as correspondence exchanged with lawyers.

Barrett J. found that the warrant issued was suitably constrained in both scope and effect, and the CCPC adopted a proportionate approach when conducting the search. However, he held that it was 'entirely unclear' how it was proportionate to the legitimate aim pursued by the CCPC for it to review the material that it was not allowed to possess during the course of the raid, without any impartial screening.

Top 10 tips to prepare for a dawn raid

Having clear internal procedures, well trained staff, and experienced counsel present during raids will help organisations to find the correct balance between cooperation and protecting privacy rights. Different regulators operate under different legislative frameworks, but the following are some tips on what to do when faced with a dawn raid:

- have a dawn raid response procedure in place so that everyone knows what to do;
- contact external lawyers and key executives and directors immediately;
- ask for each officer's proof of identity and take a copy of it;
- ascertain the team leader and the purpose of the inspection;
- check the warrant, authorisation or other formal document to ensure that it correctly identifies the business premises and the scope of the investigation;
- keep an inventory and a copy of all documents taken by the investigators;
- if correspondence with lawyers is copied or seized, object and ask that it is kept separately from other documents copied or seized and that it is not reviewed until a determination has been made as to whether it is legally privileged;
- if investigators attempt to copy or seize files or devices which contain material that is irrelevant to the matter under investigation, object and ask that those files or devices be put aside for your lawyers to discuss with the investigators after the raid;
- where agreement cannot be reached with investigators on relevant files or devices to be copied or taken, have lawyers request an independent third party to be appointed to examine the material and sift through relevant or irrelevant material: and
- co-operate with the investigators and do not obstruct or impede the investigation at any time (which may be an offence) whilst being mindful of your legal rights and the legal duties of the investigators.

Davinia Brennan
A&L Goodbody
dbrennan@algoodbody.com