Raad van State

ACA EUROPE

Colloquium organized by the Council of State of the Netherlands and ACA-Europe

"An exploration of Technology and the Law"

The Hague 14 May 2018

Answers to questionnaire: Cyprus

Colloquium co-funded by the «Justice » program of the European Union

Mr Justice Leonidas Parparinos, Supreme Court of Cyprus

ACA-Europe: An exploration of Technology and the Law

Digital decision-making

1. In an era of e-government and online government, the language of government is quickly changing. Automated, computer generated decisions have transformed the evidence-based, discretion-based decision-making process to data exchange and big data analytics. The rapid technological advancements accelerated automation in the decision-making process. Nowadays, computer systems can be used to aid or guide a human decision-maker or they may be used in lieu of a human decision-maker and they can be integrated at different stages of the decision-making process. This entails that, administrative decisions can be wholly or partly automated. Moreover, a further distinction can be made. The terms decisions and acts are commonly used interchangeably. But never before has their distinction been more paramount. The term act, has the generous ability to bring under its umbrella the plethora of modern decision-making methods and may be best fitted to describe the result of pre-programmed, computer models. That is, an act is the system's response or 'answer' to an input of information entered by a user in accordance with 'predetermined' outcomes. By contrast, many administrative decisions require and result from the exercise of discretionary powers.

Acts resulting from automated decision-making are used by Cyprus' administrative bodies mainly in the fields of tax declarations and pensions. To give an example, the Tax Department has introduced an online 'e-tax' system to help taxpayers in completing their annual assessment tax returns. At first glance, e-tax might not appear to fall into the category of automated administrative decision making. However, with each click and based on one's answers the system skips options and determines on its own which options are not relevant through the matrix of pre-programmed pathways.

The legal framework

Within Cyprus' legal order, all administrative decisions/acts can be contested and be judicially reviewed before the Administrative Court, which is the court of competent jurisdiction under *Article 146 of the Constitution*. The Administrative Court has jurisdiction to review on both points of fact and law and is not bound by the findings of the administrative body as to the facts of the case. It may, therefore, take an independent view on the facts. However, the Administrative Court cannot substitute its own decision for that of the public body. This can only be done where the decision relates to matters of asylum and tax discrepancies, in accordance with the provisions of the *Administrative Court's Act 131/2015*. In all other matters, it can only annul the decision on several grounds. Judgments of the Administrative Court can be appealed to the Supreme Court, on points of law alone.

As a general rule, administrative decisions/acts must be well and sufficiently justified (*section 26(1) of General Principles of Administrative Law Act 158(I)/1999*).

Justification must be clear and not general or vague[1]. Otherwise, judicial scrutiny is hindered. What constitutes lack of sufficient reasoning is a matter of degree and depends on the nature of each particular case[2]. The shape and extent of justification as well as the extent of details given by administration vary depending on the subject-matter and the circumstances that surround each case (*section 26(2) of 158(I)/1999 Act*). As precedent law puts it, "an administrative decision must be well-reasoned for judicial review to take place, constrained of course, to the issues upon which discretion was exercised and it is unnecessary to extend to issues of technical nature, which fall outside the jurisdiction of the Administrative Court"[3]. Automated, computerised decisions, however, fall outside the spectrum of justification. *Section 27* of the aforementioned Act 158(I)/1999 states that administrative acts issued uniformly in large numbers or mechanically or by the means of computers, do not require justification.

The reality is that the growth and application of these systems was introduced into the public law sphere well before anyone could properly reflect on how these systems interrelate with administrative law principles. The use of these systems by the government may raise questions as to the measures necessary to ensure their compatibility with the core administrative law principles that underpin a democratic society governed by the rule of law. For example, would it not be important to safeguard the transparency and accountability of government decisions by the provision of reasons for an effective judicial review? Equally, would it not be important to safeguard the legality of administration's actions? Those who purport to exercise public-decision making powers must be authorised to do so as a matter of law- *the overriding principle of legality*. Therefore, if an automated system has been utilised to make a decision in whole or in part, the use of that system must be authorised. Does a statutory authority vested in a public servant extend by implication or 'delegation' to an automated system?

Judicial review on administrative decisions is an important instrument on the control of executive power. Citizens' access to judicial review procedures raise issues relating to rules that bind them. Safeguards need to be in place in order to ensure that the individual's rights to hold decision makers to their obligation is preserved.

Discussion

Administrative justice commenced with the central, fundamental and constitutional role played by courts in checking government power. It became anchored in a constitutional separation of powers that safeguarded the role of an independent judiciary in declaring the law, checking executive error and safeguarding the citizen against government. Similarly, administrative justice developed core principles of administrative law – natural justice, good faith, the rule of law, legality, reasoned decision making, proportionality, impartiality, abuse of power, good administration

[1] Kounounas v. Republic (2001), 3 C.L.R. 1163, Marina Neofytou v. Council of Ministers and others (2006) 3 C.L.R. 768

[2] Athos Georghiades and others v. Republic (1967) 3 C.L.R. 653, Renos Kyriakides v. Republic (1976) 3 C.L.R. 364

[3] Lambrou v. Republic and others (2009) 3 C.L.R. 79

etc. On a later stage, administrative law even became an ally in making public administration more 'citizen centred'[4].

- Will the digital age require us to rethink and reposition the principles of administrative justice?

Judicial review provides a check on executive/administrative abuse, regulates the exercise of legal power, secures the rule of law and safeguards individual rights against unlawful encroachment by the government.

- Does the digital age hinder the scope and purpose of judicial review?

Digital proceedings

2. Digital proceedings include e-filing (digital case files) / e-justice and online justice. Legal proceedings in Cyprus, still maintain their traditional, paper form. Neither of the two is currently in place. The Commission's 2016 Scoreboard, has been an indicator that change needs to be in motion. By ranking Cyprus at the lower end of the spectrum with one of the lengthiest proceedings in administrative cases amongst the member states, it has raised issues for concern[5]. In the not so recent case of ***Pouyiouka and others v. Thrasyvoulou***[6] it was stated that justice delayed is justice denied. Cases should be tried as quickly as possible and judgments reserved should be issued within a reasonable time, as safeguarded by *Article 30.2 of the Constitution* and *Article 6.1 of ECHR*.

An electronic system would enable cases to be started and managed electronically. Full operation was expected within the period of two years[7] however, actions are currently at initial stages. Digitalising proceedings would definitely entail the use of an innovative and modern computer program. But, the technological infrastructure needed might outweigh the tight fiscal constraints of the government. The Government however, should commit to investing a respectable amount to modernise the courts. Furthermore, this would entail revision and amendments to the Rules of Procedure. A highly simplified procedural code will be needed to accommodate the modern methods of e-justice.

e-filing

E-filing and e-Services, have been implemented in numerous Departments of the Civil Service with beneficial outcomes. To give an example, the Department of Registrar of Companies and Official Receiver and the Tax Department have both implemented electronic filing of documents.

[4] Influential factors, among others, was the *Code of Good Administration* promulgated by the European Parliament in 2001.

[5] The 2016 EU Justice Scoreboard, European Commission and Supreme Court's Special Report, 2016

[6] (1998) 1 C.L.R. 2014

[7] Supreme Court's Special Report 2016, page 46

Implementing e-filing rules to mainstream and reduce the paper filing of legal documents would cut unnecessary paperwork and make the experience more straightforward and simpler. Actions to be debated have been initiated on the matter, for electronic filing to be introduced within Cyprus' legal system. The use of one single digital system would be highly beneficial. It would provide an online process to manage cases from filing to judgment.

The main pros and cons have been identified and a concise list has been included below:

Advantages	*Disadvantages*
• Saves time, money, and transportation costs • Reduces delays in retrieving court documents • Enhances virtual filing accessibility from the convenience of home or the office • Enables lawyers and court clerks to work more efficiently by reducing the time and effort needed to manage case files • Allows most legal professionals (lawyers and paralegals) to receive notices, orders, and judgments from the court electronically • Eco-friendly	• Software and hardware malfunctions • Additional investment in secure computer security and software to make sure documents are protected and properly formatted • No personalised service with the court's registry upon filing the documents • Computer hacking

Online justice

The resolution of cases has historically revolved around advocacy before a judge in a physical courtroom. Online justice means that some cases may be handled entirely online rather than in courtrooms. Many foreign jurisdictions have adhered the idea of online justice, for example, for cases of lesser severity / significance to be dealt with quickly or on the basis of papers submitted to the court electronically.

Objectives of online justice

1. Frees the judiciary to spend their time considering the cases that need their attention most.
2. A modern justice system must be proportionate. The cost, speed and complexity should be proportionate to the scale and substance of the case.
3. Online justice should not be obligatory because the justice system should be accessible to everyone. Online or traditional proceedings should be used as best meets the circumstances of the case. This means that access to courts ought to be available and intelligible to non-lawyers and at the same time, to

people who are not comfortable with new technology or even the small core of non-internet users who must be supported through the traditional procedure.

With these in view, one may argue that administrative jurisdiction, appears prima facie, to be a good example for online justice implementation because pleadings are conducted in writing and oral submissions are kept to a minimum in the entirety of the procedure.

A concise overlook is provided below to demonstrate the current judicial review procedure for a better understanding:

Procedure before the Administrative Court- first instance: Pleadings and procedure are governed by the *Administrative Court (No.1) Procedure Rules of 2015 and Supreme Constitutional Court Procedure Rules of 1962.* Once pleadings have been submitted, written statements/skeleton arguments would need to be submitted in turn for advocacy submissions to be made thereafter. The administrative file is submitted to court at this latter stage.

Procedure before the Supreme Court- last instance: Pleadings are governed by the *Appeals (Judicial Review Jurisdiction) Procedure Rules of the Supreme Court of 1964*. Preliminary procedure and hearing are governed by *Appeals (Preliminary procedure, Skeleton arguments, Advocacy time limits and Summary procedure for striking out manifestly unfounded appeals) Procedure Rules of 1996*. During the preliminary procedure, all skeleton arguments are submitted within the time frames specified by the Procedure Rules, unless the Court directs otherwise. Time frames may be abridged if the court thinks fit. Under *Rule 5 of the Procedure Rules of 1996*, the Supreme Court has the power to enter a case for hearing without undertaking a preliminary procedure, whenever the court considers it to be just. However, the need for an expedient trial on the appeal is no reason for not following the preliminary procedure stage. Only where there are founded reasons for circumventing the procedure, will the Court regard it just to do so. A party to the proceedings may apply for such circumvention to the competent Registry[8].

However, *Article 30 of the Constitution* enshrines **judicial protection.** *Article 30.1* acknowledges one's right for the unimpeded access to the court for the assertion or vindication of his rights. *Article 30.2* specifies that in the determination of one's civil rights and obligations or against any criminal charge faced, a person has the right to a fair and public hearing within a reasonable time by an independent, impartial and competent court, established by law, identical to Article 6.1 of ECHR. Furthermore, *Article 158 of the Constitution* envisages the establishment by law of courts subordinate to the superior court in sufficient numbers for the undelayed administration of justice and the efficient application of human rights.

Transferring justice online will raise questions of transparency, fairness and openness encroaching on the fundamental and constitutional right of a fair and public hearing by an independent and impartial court. Justice should not only be done, but should manifestly and undoubtedly be seen to be done [9]; the common law

[8] Supermarkets Association and others v. Republic (1997) 3 C.L.R. 142

[9] Lord Chief Justice Hewart's dictum *in R v Sussex Justices; Ex parte McCarthy [1924] 1 KB 256, 259*

dictum that supports a requirement of judicial impartiality and extends beyond the common law world.

Digital dispute settlement in the public sector without involving the courts

3. It is indeed true that unnecessary escalation of disputes should be emphatically discouraged and kept out of the courts whenever possible. Supporters claim that Artificial Intelligence (AI) technologies can do exactly that and more. AI means machines can do more than follow very specific instructions, performing tasks that formerly depended on human reasoning like IBM's Watson – an AI computer system which helped diagnose and recommend treatment for leukemia in a patient whose case had been baffling doctors for months. The machine studied the patient's medical information and, in ten minutes, was able to cross-reference her condition against 20 million oncology records. These machines can identify patterns, evaluate data, and learn from new information.

However, Cyprus' legal and judicial system is unfamiliar with the world of AI or algorithmically-organised systems for the settlement of disputes prior to the commencement of proceedings or during the adjudication process. Only databases and search engines like Leginet and Cylaw are widely used which resemble many legal portals available throughout the legal world. However, a Leginet/Cylaw type system does not even "know" which side won the dispute or with respect to which claims or issues.

The common-law system, based on the principle of *stare decisis* means that the judiciary should assign similar outcomes to similar cases[10]. The doctrine of precedent law is a fundamental pillar of law, interlinked with *legal certainty* (predictability) and the *rule of law*[11]. However, even stare decisis allows for some narrow margins of divergence when certain conditions are met. Quite notably, in the sphere of administrative law those narrow margins widen if entrenched constitutional and administrative principles are at stake, e.g. the doctrine of separation of state powers.

It can, therefore, safely be said that the goal of a computerised model would be exactly that, to resemble the doctrine of *stare decisis*. However, biases exist in algorithmically-organised systems. Typically, government departments and institutions do not write their own algorithms, they buy them from private companies. The algorithm creators, even if they strive for objectivity and neutrality, build into their creations their own perspectives and values. Also, datasets to which algorithms are

---

[10] Ronald Watts and others v. Laouri and others, Civil Appeal 319/2008, 7/7/2014 (majority ruling), Republic v. Demetriades (1977) 3 C.L.R. 213, 263-264, Nicolaou and others v. Nicolaou and others (No. 2) (1992) 1B C.L.R. 1338, 1405-1406, Republic and others v. Yiallourou and others (1995) 3 C.L.R. 363, 373-374, Mavrogenis v. House of Representatives and others (No. 3) (1996) 1 C.L.R. 315, 332-337, Koulounti and others v. House of Representatives and others (1997) 1B C.L.R. 1026, 1105, Vironas v. Republic (1999) 3 C.L.R. 77, 85, Christos Hadjikyriakou Properties Ltd v. Republic (2001) 3B C.L.R. 901, 905, Antenna TV Ltd and others v. CY.T.A. and others (2002) 3 C.L.R. 793, 809-811, Panayides Contracting Ltd v. Charalambous (2004) 1A C.L.R. 416, 488 and Investylia Public Company Ltd v. Tseriotis, Civil Appeal 9/2009 and 10/2009, 13/3/2013

[11] Ronald Watts and others v. Laouri and others, Civil Appeal 319/2008, 7/7/2014 (majority ruling), Republic and others v. Yiallourou and others (1995) 3 C.L.R. 363

applied have their own limits and deficiencies. Would such systems be able to accommodate the exceptions of the doctrine? Moreover, what about open-to-interpretation laws. These laws can yield more than one possible outcome, especially in the absence of hard precedent. For example, laws that include concepts of 'fit and proper', 'good faith' and 'proportionality'.

If such systems were part of the adjudication process they would lead in a constructive failure to exercise juridical thought since they would apply predetermined outcomes which may be characterised as pre-judgment or bias. It is settled law that each case is decided upon its own merits aided by precedent law. The traditional common law approach has the advantage that judges can express themselves precisely as they so wish. They have the liberty to dissent as they see fit, or to concur for different reasons of their own. But, more importantly, judges express their own reasoning in their judgments. In ***Investment Group of "Lefkonikou" Co-Operative Ltd v. Lofiti***[12], the Court highlighted the structure and style of judgment writing which as enshrined in *Article 30.2 of the Constitution* and precedent law, must be well-reasoned. This entails the correct determination and consideration of trial issues, a summary of substantive evidence, its correlation with the findings and conclusions drawn as well as the with the verdict of the Court[13]. A judgment is read in its entirety. It is the Court's obligation to evaluate all evidence admitted and to draw conclusions on all contested issues, in order for the judgment to include the necessary juridical thought on all disputed issues[14].

Also, pre-determined outcomes are not compatible with judges' independence. In the recent judgments of ***Kyprianou v. Police***[15] and ***Patsalides v. Police***[16] the Supreme Court stated: "It is settled precedent law that the style of writing, the wording and the expression of opinion of every judge is protected and documented as a fundamental value of his independence. However, this freedom is rule-guided. It is a judge's obligation to include in his judgment all that is necessary for one to comprehend the juridical thought behind it…".

The law is an evolving, living, organism and our existing systems have checks built into them that would need to be replicated in any new system. When superior courts grapple with cases without clear precedents, they are engaged in a process that determines, declares, clarifies and interprets the law. This kind of evolution is a central tenet of common law systems and allows for instantaneous responsiveness to changing mores. If legal reasoning were automated, it must be demonstrated that this responsiveness would not be lost. Before embracing the new world and its new entries, we must make sure not to lose things hard fought to establish and protect.

Technology-neutral legislation

4. It should be stated from the outset that examples given in this part of the questionnaire do not derive from any kind of legislative advisory role of the Supreme

[12] Civil Appeal 42/2011, 7/7/2017
[13] Kannaourou and others v. Stadioti and others (1990) 1 C.L.R. 35
[14] Christodoulou v. Aristodemou (1996) 1 C.L.R. 552
[15] Criminal Appeal 50/2016, 19/7/2017
[16] Criminal Appeal, 87/2015, 20/1/2017

Court, since the Supreme Court of Cyprus is not an independent advisory body with a general advisory function, such as the Council of State and does not review technical aspects of the legislation, feasibility and language[17].

It is indeed true that, the desirability of technology neutral legislation became paramount without being questioned. Alarmingly, legislators seem to be unaware of what the term "technology neutrality" actually means since it does not appear to have a universally accepted definition. Different interpretations arise. Technology neutrality could mean for example that legislation should not refer or require a particular technology for its implementation. Technology neutrality is one of the key principles of the European Regulatory Framework for electronic communications. In this sense, it means that the same regulatory principles should apply regardless of the technology used, that is that the fundamental principles of regulation remain the same whatever the medium (principle of technological neutrality)[18]. But, outside the telecommunications sector, it could also mean that certain rules should apply online as well as offline, that is applying identical rules and hence equivalent treatment, to different technologies. Furthermore, technology neutrality is interconnected with the aim and purpose of the statute.

Nowadays, due to the rapid developments in the ICT sector the law finds itself unable to keep up pace. The enactment of technologically neutral legislation provides the opportunity needed for the law to catch up. Technology neutral legislation is futureproofing and forward looking in ensuring flexibility to future technological developments and avoids unnecessary and over-frequent revision.

Some laws are indifferent to the technology involved. The law of premeditated murder[19] or manslaughter[20] are obvious examples because they apply to the behaviour of those involved and the effects of that behaviour. They are indifferent to the means through which those involved behave or by which those effects come about. Also, in the information and communications technology field, copyright law[21] is one of the most clearly technology neutral / indifferent statutes since it is focused on the nature of the use of the work rather than the medium by which the use is accomplished.

Other statute laws, are framed in a way that do not favour one or more technology implementations over others. Such an example can be provided by the EU Directive on Electronic Signatures[22] which was transposed into national law. The definition of electronic signatures included in the *Legal Framework for Electronic Signatures and*

[17] The Supreme Court's advisory role is limited to a structural, preventive scrutiny on the constitutionality of a Bill or Act alone, under *Article 140 and Article 137 of the Constitution*. In essence, the President of the Republic may refer the Bill/Act to the Supreme Court for an opinion on constitutional issues. Constitutionality in this context entails a thorough examination of the Bill's/Act's compatibility with the constitution as well as with EU law and extends to well entrenched constitutional principles, such as separation of powers, natural justice (*audi alteram partem*), proper administration and human rights. However, the Supreme Court does not examine the consequences the Bill/Act in question will have in the 'legal sphere' once in force.

[18] CY.T.A. v. Office of Electronic Communications and Postal Regulations, Case No. 326/2007, 11/5/2009

[19] Section 203 of the Criminal Code, Cap 154

[20] Section 205 of the Criminal Code, Cap. 154

[21] Intellectual Property Right and other Related Rights Act of 1976, 59/1976

[22] Directive 1999/93/EC on a Community Framework for electronic signatures

Miscellaneous Provisions Act 2004 188(I)/2004, which reproduced the Directive almost verbatim, provides an example of a technologically-neutral definition. An electronic signature means data in electronic form which are attached to or logically associated with other electronic data and which serve as a method of authentication. This is a technologically neutral and a broad definition as rapid technological development and the global character of the internet necessitate an approach which is open to various technologies and services capable of authenticating data electronically.

In many cases the online position may be so different in kind from their offline counterparts that it might not be possible to identify how equivalent treatment might apply. In the case of ***Sotiris (Akis) Papasavva v. Fileleftheros Public Company Ltd and others, Civil Claim 9493/2010, 27/3/2010***, which concerned an online defamation claim, the court ruled in favour of the application for a preliminary ruling to the CJEU since it was necessary for the court to decide whether the defamation provisions of *sections 17-25 of Civil Liabilities Act, Cap. 148* applied equally to online defamation claims and if so to what extent were *Directive 2000/31/EC* and the *Act 156(I)/2004*, which transposed the aforementioned Directive, applicable to such cases. The CJEU on 11/9/2014 ruled that Directive 2000/31/EC does not preclude the application of rules of civil liability for defamation. Also, the limitations of civil liability specified in *Articles 12 to 14 of Directive 2000/31/EC* do not apply to the case of a newspaper publishing company which operates a website on which the online version of a newspaper is posted, that company being, moreover, remunerated by income generated by commercial advertisements posted on that website, since it has knowledge of the information posted and exercises control over that information, whether or not access to that website is free of charge. The limitations of civil liability specified in Articles 12 to 14 of Directive 2000/31 are capable of applying in the context of proceedings between individuals relating to civil liability for defamation, where the conditions referred to in those articles are satisfied[23].

5. As precedent law puts it, “the wording of a legislative provision is both the starting point as well as the limit to all interpretational attempts. Where the wording is clear, the natural and regular use of the word is attributed”[24]. “The purpose of interpretation is to find the intentions of the lawmaker”[25]. Indeed, legislation based on specific technology can quickly become outdated, but the problem with technology neutral legislation is that questions arise as to whether and where the new advance technology falls within the spirit and the intent of the lawmaker. It is appropriate for one to expect the committal of a further debate and subsequent decision about the newly introduced technology. Hence, when a statute is technology specific, the intention of the lawmaker is exactly that.

[23] C-291/13, 11/9/2014

[24] Ghalanos Distributos Ltd v. Republic (2002) 3 C.L.R. 528, G.P.B. Hunting Ltd v. Police, Criminal Appeal 122/2015, 8/5/2017

[25] Theofanous and others v. Central Bank of Cyprus (2002) 3 C.L.R. 384, Hotel Enterprises Plaza ltd and others v. Yermasoyia Improvement Council (1998) 3 C.L.R. 348, G.P.B. Hunting Ltd v. Police, Criminal Appeal 122/2015, 8/5/2017

Digital enforcement

6. Digital Tachographs used as control devices for recording drivers' activities, such as driving and rest periods are also used in Cyprus. They were made mandatory by Regulation 1360/2002 which amended Regulation 3821/85. The Digital Tachograph allows for the effective and efficient enforcement of drivers' activities including speed limit violations.

Also, digital surveillance cameras are used by law enforcement authorities to identify violators of speed limits. *Section 6* of *Automobiles and Road Traffic Act 86/1972* makes it an offence to disregard speed limits. In order for the police to efficiently enforce the provisions of the statute they are aided by digital surveillance cameras predominant to roads where over-speeding is frequent.

Law enforcement is by its nature, an information-rich activity. Law enforcement activities in the collection and analysis of information can be broken into three categories:

1. To determine that a law has been violated
2. To determine the identity of the person or persons responsible for a violation of law
3. To enable a case to answer in court; that is that the person or persons identified in fact were guilty of the violation.

All of these activities of the police have been altered by advancements in technologies that have become available for collecting, storing, processing and manipulating data.

However, digital data often includes personal data. Questions arise as to how long these data can be retained by an authority, data protection considerations, privacy and in extent the future of the right to digital privacy. Any action into people's personal data, digital or otherwise, must be properly authorised by a court order and must be limited to what is absolutely necessary to achieve a legitimate purpose. Also, authorities that collect personal information must protect it and respect people's right to privacy and correspondence/communication.

Within Cyprus' legal order, personal data is protected by *Personal Data Protection Act of 2001 (Protection of Natural Person) 138/2001*. The statute protects the privacy and all personal data collected for or about citizens, especially as it relates to processing, using or exchanging such data. Most importantly, the provisions of the statute apply to public authorities, semi-governmental organisations and to the private sector, equally. In accordance with the provisions of the statute, personal data, inter alia:

- should not be disclosed or shared without explicit consent,
- data collected should only be used for legitimate purposes,
- once collected personal data should be kept safe and secure,
- persons have access to their personal data and are allowed to correct any inaccuracies and

- the combination of personal data filing systems between authorities is only permitted under certain conditions with the prior acquisition of a 'combination of filing systems license' from the Commissioner of Personal Data Processing.

Furthermore, *Article 8 of ECHR* protects the right to respect for private and family life. Everyone has the right to respect for his private and family life, his home and his correspondence and there shall be no interference by a public authority except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

Similarly, *Article 15 of the Constitution* safeguards the right to respect one's privacy and family life and there shall be no interference except as is in accordance with the law and is necessary in the interests of national security or constitutional order or public safety or public order or for the protection of health or morals or for the protection of the constitutional rights and freedoms of others or transparency in public life or for the prevention of corruption in public life.

Moreover, *Article 17 of the Constitution* safeguards the right to respect and protect one's correspondence and any other kind of communication. *Article 17.2C*, in particular, provides that no interference is allowed in the exercise of this right except as in accordance with the law, after a court order is issued in accordance with the provisions of the law for the investigation or prosecution of a serious criminal offence punishable with imprisonment of 5 years and more and interference concerns communication data necessary to identify an individual user or to provide information about their online activity. *Article 4* of the *Retention of Communication Data for the Investigation of Serious Criminal Offences Act of 2007 183/2007*, which transposed *Directive 2006/24/EC*, makes provisions for the issuance of such court orders for the disclosure of such personal, communication information. Once a court order is issued the relevant Communication Organisation must disclose the information, otherwise under a duty to keep confidential, safe and secure.

In order to illustrate the point, *Directive 2006/24/EC*, creates an obligation for the Member States to introduce a system for retaining traffic and location data for six months up to two years for the purpose of investigation, detection and prosecution of a serious crime. The Directive allowed for a degree of diversity amongst the Member States depending on the intensity of reactions at national level about privacy erosion. It came under the judicial lens in the joined cases of ***Digital Rights Ireland and Seitlinger and Others***[26]. The CJEU held that the Directive did interfere with the right to privacy by imposing a duty to retain data accessible to public authorities[27]. However, the Directive did not violate the essential core of the right to privacy since access to the content data was prohibited. The same applied as to the right to data protection where there is an obligation to monitor the way in which the retained data are kept. A further point made was that the interference did satisfy a general interest objective worth pursuing in a democratic society. Combating and preventing a

[26] C-293/12 and C-594/12
[27] §34 and 35

serious crime was held to be a valid manifestation of the general interest[28]. Ultimately, the CJE applied the proportionality test and held that, the Directive 2006/24/EC on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and which amended Directive 2002/58/EC was invalid.

As already mentioned Cyprus implemented the said Directive in its legal order[29]. *Act 183/2007* applies to any crime punishable with imprisonment of 5 years and over. The constitutionality of *Act 183/2007* was examined by the Supreme Court in the case of ***Alexandrou (2010) 1 C.L.R. 17.*** The case concerned an application for leave for *certiorari.* As a result of the Supreme Court's judgment in ***Alexandrou***, Parliament amended Article 17.2 of the Constitution. The result of the amendment is that interference with the right to privacy can now include access to communication data retained after a court order is issued for the investigation or prosecution of a serious criminal offence punishable with imprisonment of 5 years and over and interference concerns communication data necessary to identify an individual user or to provide information about their online activity.

[28] §41-44

[29] Retention of Communication Data for the Investigation of Serious Criminal Offences Act of 2007 183/2007