

# **From Reality to Virtuality: The New Forms of Power and Governance in the Information Society**

Godwin Darmanin (Sofia University St. Kliment Ohridski)

## **Abstract**

This paper philosophically examines the social, the political and the technological processes that are found within the 'Information Society' in relation to the new forms of governance, power, democratic tools, privacy and globalisation. I first start my essay by scrutinising the role of the nation state in the 'Information Society' in order to determine whether in the latter, governance has become more problematic. Subsequently, I define and depict both e-Democracy and e-Government with the aid of topical examples and also explain that although the two terms are related, they do not refer to the same thing. Following that I examine the processes of globalisation and illustrate how these are affecting both established information societies but also those nations which are still not considered to be fully fledged information societies. Afterwards, I also discuss how the 'Information Society' supports citizens' privacy when at the same time it permits the proliferation of new forms of technologies which can be easily used for mass surveillance. Finally, I also discuss whether or not in information societies, national governments still hold the ultimate power. All of these topics are comprehensively discussed in order to determine whether or not the nation state is still relevant in today's information age.

## **I. Introduction**

As of the end of 2010, the United Nations has a total of 192 member states. Moreover, a number of regional alliances such as the EU, EFTA, AU, APEC, and ASEAN all together comprise many member states in political and/or economic unions. Within the individual nation states themselves, one also finds regional or local groupings such as the individual states which make up the USA and the Italian *regioni*. At the same time, one also finds a

number of multi national corporations (MNCs) and non-governmental organisations (NGOs) that operate both from within and also across the various nation states.

It must also be noted that all of the 192 UN member states claim to be sovereign, which means that they have the power to exercise supreme and permanent authority over their territories. In spite of this, and because of the fact that most of them are members of political and/or economic unions, in practice they possess only varying degrees of political sovereignty. This observation is even more accentuated by the fact that their same sovereignty is kept in check by NGOs while at the same time MNCs put a lot of pressure onto the governments so that the latter can safeguard their economic interests.

The framework which has been depicted so far can only operate through various processes of globalisation and which, in turn, are backed up by the processing of information. As a matter of fact, MNCs can transfer their capital efficiently thanks to present-day information technologies. At the same time NGOs are in a position to organise and co-ordinate both their local and international activities efficiently thanks to the same information technologies. Political and economic unions are also totally dependent on the processing and the dissemination of information and for instance the EU officially proclaims that it (and as a result also its citizens) belong to the “information society”. Consequently, the information age and the information society have further accentuated pressure on both the power and on the authority of those governments whose nation states are information societies. At the same time it is perhaps also the case that a lack of information and of knowledge have left certain governments (those whose nation states are still far from being information societies) with unlimited power to exercise their authority.

These are all themes (the nation state, power, governance, and globalisation) that I will be discussing throughout this paper. This is mainly going to be done in order to ascertain whether or not the nation state is still relevant in the information society and to try to determine who holds the power in a liberal and democratic information society, which is at times bewildered by the virtuality that is created by its technologies. Moreover, all of this is going to be done without neglecting the issues of both privacy and surveillance because whereas most citizens of the information society rightly believe that they are entitled to their privacy, at the same time their

governments are still keen to pursue some policies of surveillance!

## **II. The role of the “nation state” in the information society**

It can be confidently stated that it has never been easy for authorities that preside over nation states to exercise their power and to manage all of the activities which occur within their national boundaries. Likewise, it has never been easy for these same governments to control what goes in and what goes out of their national jurisdictions. However, it can also be observed that with the advent of the information age, all of the governmental tasks which were already not easy to handle, have even become more problematic. For instance, before the introduction of today's taken-for-granted information technologies, it was easier for governments to control the inflow and outflow of money. Similarly, it was also easier for governments to monitor and control the activities which used to take place among their people and the activities which used to take place between the latter and the people residing in other nations. In this regard Johnson and Post have eloquently observed how

The rise of the global computer network is destroying the link between geographical location and: (1) the power of local governments to assert control over online behaviour; (2) the effects of online behaviour on individuals or things; (3) the legitimacy of the efforts of a local sovereign to enforce rules applicable to global phenomena; and (4) the ability of physical location to give notice of which sets of rules apply. The Net thus radically subverts the system of rule-making based on borders between physical spaces, at least with respect to the claim that Cyberspace should naturally be governed by territorially defined rules.<sup>1</sup>

Each of these four points delineates the areas of major concern for governments in information societies and consequently each of Johnson's and Post's remarks need to be discussed before progressing further.

---

<sup>1</sup> David Johnson and David Post, “Law and Borders: The Rise of Law in Cyberspace”, *Stanford Law Review*, Volume 48, Number 5, pp. 1367-1402 (May, 1996).

### **The power of local governments to assert control over online behaviour**

Before the commercialisation of the Internet, people living anywhere in the world, even in those nations which towards the end of the 20th century were already considered information societies, did not have real opportunities to voice their opinion without being restrained through both explicit and implicit degrees of control. Hence, even though in the information societies of the pre-Internet period, people could write letters to the editors of daily or weekly newspapers, and they could participate in television and radio phone-ins, their opinions could never really be voiced unless this conformed with certain rules of behaviour as implicitly set by society, and with the agendas of the broadcaster or publisher (both public and private). All of this changed overnight once more and more people started to connect to the Internet. As a matter of fact, in cyberspace people started to utilise a myriad of tools such as forums, newsgroups, and personal websites to post personal opinions, images and also audio and video clips pertaining to every imaginable topic. Among all posted material, one can even to this day find content which ranges from the questionable to the outright illegal. Faced with such a situation, governments reacted mainly by setting up apposite sections within the police corps so that the latter can take action against the perpetrators of what is now being defined as cybercrime. However, this kind of control over online behaviour has never been easy to carry out, mainly because the cybercrime police are usually behind in relation to both technologies and know-how when compared to those responsible for the online criminal acts. Moreover, even when the police manage to apprehend those responsible, it is usually difficult for them to take legal actions against the perpetrators unless the law already caters for such occurrences. Another difficulty arises in relation to geographic locations, since even if local law caters for questionable online behaviour, in certain occasions no action can be taken against the perpetrators since the servers which host the questionable content are located outside the local government's jurisdiction. It must be noted that governments in the most advanced information societies are now doing their best to catch up with such situations; however, they are still rather limited whenever they try to assert control over online behaviour.

### **The effects of online behaviour on individuals or things**

The Internet has certainly brought about both positive but also negative effects on individuals or things. The former are definitely numerous and these range from online education up to the possibility to interact with friends or relatives who live in remote geographical locations. However, the Internet has also created negative effects vis-à-vis human behaviour which once again governmental authorities are finding difficult to control. Two such effects are cyber-bullying and cyber-stalking. The UK government states that the former occurs “when one person or a group of people try to threaten, tease or embarrass someone else by using a mobile phone or the Internet”.<sup>2</sup> As regards cyber-stalking, Jaishankar and Sankary state that it “is a new form of computer-related crime occurring in our society. Cyber stalking is when people are followed and pursued online. Their privacy is invaded, their every move watched. It is a form of harassment that can disrupt the life of the victim and leave them feeling very afraid and threatened.”<sup>3</sup> Besides affecting individuals, online behaviour has also affected things such as the mass media, with the latter having to adapt as a consequence. For instance, all television and radio networks as well as newspapers have an online presence and this is not limited to having only a website. Nowadays, the mass media have also infiltrated into social networking websites such as FaceBook, and as a consequence the mass media have increasingly become multi-dimensional. These and similar effects of online behaviour on individuals or things have certainly rendered the role of the nation state in the information society less effective, even though it must be noted that in most information societies, governments are trying to deal with such effects as efficiently as existing technology and legislation currently permits them.

### **The legitimacy of the efforts of a local sovereign to enforce rules applicable to global phenomena**

To illustrate the third point of Johnson and Post we must first

---

<sup>2</sup> [www.direct.gov.uk/en/YoungPeople/HealthAndRelationships/Bullying/DG\\_070501](http://www.direct.gov.uk/en/YoungPeople/HealthAndRelationships/Bullying/DG_070501)

<sup>3</sup> K. Jaishankar and Uma Sankary, “Cyber Stalking: A Global Menace in the Information Super Highway” in *ERCES Online Quarterly Review*, Volume 2, Number 3 (July - September, 2005).

understand what global phenomena are. Put simply, global phenomena are occurrences which currently have or which will eventually have the potential to affect the entire planet and consequently all of humanity. Climate change, the problem of refugees and the destruction of the rainforest are all examples of global phenomena. Within the context of the information society, the application of information and communication technologies is a relevant global phenomenon which deserves our immediate attention. In this regard if we take once again the example of the Internet, which is certainly a global phenomenon, we can ask whether those local governments that are enforcing censorship on Internet content are justified in doing so. For instance “Reporters without Borders” lists twelve countries in its latest “Enemies of the Internet” list and states that “Some of these countries are determined to use any means necessary to prevent their citizens from having access to the Internet”. The same organisation furthermore illustrates the situation in each of these countries and for instance in relation to Egypt states that “Since early 2007, the government has been reinforcing Web surveillance in the name of the fight against terrorism, under the iron fist of a special department of Egypt’s Ministry of Interior”.<sup>4</sup> In this instance the main argument put forward by “Reporters without Borders” is that Egypt wants to restrict access to information and to deny freedom of speech under the false pretence that it is trying to safeguard its national interests from terrorist attacks, and this is indeed a clear case of a local government which is enforcing rules applicable to global phenomena. Nevertheless, questions remain as to whether this is a legitimate course of action in view of the fact that Egypt is after all a sovereign nation state and that consequently its government has overall authority over its population.

### **The ability of physical location to give notice of which sets of rules apply**

The fourth and last point that Johnson and Post put forward is the ability of physical location to give notice of which sets of rules apply. To illustrate this point we can refer to the case of Second Life, a popular virtual

---

<sup>4</sup> Reporters Without Borders, “World Day Against Cyber Censorship”, New Media Desk (March 12th, 2010).

word which can be accessed on the Internet. The user's manual states that "You have the ability to do almost anything here, but there are basic rules set by Linden Lab. Those rules are described in the Community Standards. Real life laws still apply in a virtual world. Linden Lab is based in California, USA, so their local laws apply to it, and your local laws apply to you".<sup>5</sup> In this particular case, Second Life is a virtual world which is located on physical servers which are physically located in California. Hence, in this case which sets of rules should apply to those users who do not physically reside in California? Matters could indeed become further complicated if we take into consideration the physical location of the same users. So, in this case, which sets of rules should apply? Those where the users are physically located or those where the virtual world is located? These and similar dilemmas are indeed extremely intricate and any government will surely not find it easy to determine which sets of rules to apply in such circumstances.

In relation to what has been discussed so far, Johnson and Post also assert that

...efforts to control the flow of electronic information across physical borders - to map local regulation and physical boundaries onto Cyberspace - are likely to prove futile, at least in countries that hope to participate in global commerce. Individual electrons can easily, and without any realistic prospect of detection, 'enter' any sovereign's territory. The volume of electronic communications crossing territorial boundaries is just too great in relation to the resources available to government authorities.<sup>6</sup>

Hence, way back in 1996, Johnson and Post had already predicted that any attempt by governments to control the flow of electronic information was going to be ineffective, and although time has mostly proved them right, the latest report by "Reporters without Borders" just proves that some governments are still persisting with their efforts to apply stringent controls. Nevertheless, one can also observe that ten out of twelve countries that have

---

<sup>5</sup> Source: Second Life User's Manual: [http://wiki.secondlife.com/wiki/User's\\_Manual](http://wiki.secondlife.com/wiki/User's_Manual)

<sup>6</sup> Johnson and Post, op. cit.

been included in the latest “Enemies of the Internet” list (Burma, North Korea, Cuba, Egypt, Iran, Uzbekistan, Syria, Tunisia, Turkmenistan, and Vietnam)<sup>7</sup> are not eager at all to take part in global commerce. On the other hand the other two countries in the list (Saudi Arabia and China) seem to favour partial participation vis-à-vis global commerce. Moreover, as one can evidently notice, no governments from the advanced economies have been included in the list since none of these can hope to hinder global commerce, even in those cases where there is the genuine need to protect the local industry.

When one takes into consideration what I have been so far illustrating, the picture does certainly not look encouraging given the role of the state in the information society. Indeed, it looks like the state is becoming increasingly helpless at least when it comes to administering the flow of products, information, and services. It is also becoming increasingly apparent that the citizens of the information society can in many instances circumvent the authority of local powers and this can be done through both legal but also through questionable ways. However, in relation to this, Christopher May observes that

By ignoring the continuing capacity of the state, much discussion of the information age fails fully to appreciate the importance of the relationship between state and citizen. Furthermore, having been told repeatedly that the state is in decline, or outmoded, many users may fail to perceive the impact governmental actions could have on them. When the state’s role in the information age is ignored or downplayed, governments are left a freer hand to indulge in the sorts of action which should be held more democratically accountable than they are.<sup>8</sup>

Indeed May’s observation poses a present and real danger in the information society because the “informed” citizen is increasingly feeling falsely liberated from the shackles of local authorities. As a matter of fact, while in the pre-digital times, all citizens were highly dependent on the

---

<sup>7</sup> Reporters Without Borders, op. cit.

<sup>8</sup> Christopher May, *The Information Society: A Sceptical View*, Polity Press, 2002.

information and on the services that only their governments could provide them with, the information society has by now advanced to such a stage where citizens have certainly the ways and means to find much of the needed information by themselves, even if the latter can in certain instances prove to be either misinformation or disinformation. As a consequence, governments might start to experience a sense of detachment from their independent citizens with the result that they might become less accountable for any of their actions. But to counter-balance this phenomenon the same, the information society is providing its citizens with two relevant mechanisms: E-Democracy and E-government and these two will be the next two topics to be discussed.

### **III. E-democracy and increasing the transparency of the political process**

One of the main pillars of any democracy is the possibility for all citizens to keep their governments in check, but for this to be really possible a number of effective mechanisms need to be in place. In the information society one such mechanism is electronic democracy. According to Trechsel et al,

E-democracy consists of all electronic means of communication that enable/empower citizens in their efforts to hold rulers/politicians accountable for their actions in the public realm. Depending on the aspect of democracy being promoted, e-Democracy can employ different techniques: (1) for increasing the transparency of the political process; (2) for enhancing the direct involvement and participation of citizens; and, (3) improving the quality of opinion formation by opening new spaces of information and deliberation.<sup>9</sup>

Each of these three points is now going to be illustrated.

Present-day political processes can indeed be bewildering for the vast majority of citizens. While most of the processes themselves are

---

<sup>9</sup> Alexander Trechsel et al., "Evaluation of the Use of New Technologies in order to Facilitate Democracy in Europe: E-Democratising the Parliaments and Parties of Europe" University of Geneva & Florence (October 8, 2003).

intrinsically convoluted, this issue has in this day and age become further complicated by most citizens' apathy towards politics and by their inclination to prefer pleasure-seeking activities. Nevertheless, a number of governments have taken the initiative to expose parts of the process to the general public. A case in point is [www.Parliament.uk](http://www.Parliament.uk), a website owned by the British government and which contains information on the parliament's role, elections and voting, the making of laws, and parliamentary sovereignty. On the same website one can also find both live and recorded transmissions of parliamentary sessions and these can be watched through the appropriately called Parliament TV. A similar service is available in New Zealand since July 2007 and it is not being excluded that similar services exist in other countries. Indeed, this is an instance where one can observe the information society delivering its best.

### **Enhancing the direct involvement and participation of citizens**

Apart from an acute apathy towards politics in general, many citizens in information societies have apathy towards elections in particular. A direct consequence of this phenomenon is low voter turnout during elections. For instance, the average EU turnout for the European parliamentary elections has dropped from 61.99% in 1979 to 43% in 2009.<sup>10</sup> In this regard, in September 2000 the European Union embarked on a trial project that was aptly called Cyber Vote. At the end of the project a two-page information sheet summarised the project as follows:

As new information and communications technologies are transforming the meaning of democracy in Europe and globally, the Cyber Vote project sought to develop a secure cyber voting system enabling European citizens to vote through their mobile phones and PCs connected to the Internet. This contributed to increase the overall participation of European citizens to all kind of elections, and more specifically the participation of the young, the physically handicapped people (including elderly), immigrants, and socially excluded people.<sup>11</sup>

---

<sup>10</sup> [www.europarl.europa.eu/parliament/archive/elections2009/en/turnout\\_en.html](http://www.europarl.europa.eu/parliament/archive/elections2009/en/turnout_en.html)

<sup>11</sup> [www.ec.europa.eu/information\\_society/activities/egovernment/docs/project\\_syn](http://www.ec.europa.eu/information_society/activities/egovernment/docs/project_syn)

Nevertheless, despite these claims, electronic voting has been plagued with documented problems since its inception and in general it has always been viewed with a certain degree of suspicion. For instance, in an article published in *The Guardian*, Wendy Grossman stated that “Democracy is made difficult by the fact that electronic voting systems are inherently flawed - and susceptible to fraud”.<sup>12</sup> Hence, although electronic voting is certainly a step in the right direction, a lot needs to be done until it gains widespread acceptance from the majority of citizens in information societies.

### **Improving the quality of opinion-formation by opening new spaces of information and deliberation**

The last point mentioned by Trechsel et al can be implemented through various mechanisms. One of these is mentioned by the Council of Europe which observes that

One of the universal complaints one hears about contemporary democracies is that they are remote. Their operations are so complex and take place through the intercession of so many layers of decision making and policy implementation that the ordinary citizen feels incapable of reaching those responsible - even when he is sufficiently motivated to do so. Moreover, the sheer volume of information that governments put out has increased to such a degree that no one can be expected to keep up unless they make an extraordinary effort.<sup>13</sup>

In this regard the same Council of Europe proposes the introduction of Democracy Kiosks so that these can offer among other services face-to-face advice from local functionaries about laws and regulations. Unfortunately, I suspect that for the foreseeable future we will not be seeing such democracy kiosks across all cities, towns and villages of the European Union, but if one day that eventually happens it will indeed mark a big step towards the

---

psis/syn\_cybevvote.pdf

<sup>12</sup> Wendy Grossman, “Why machines are bad at counting votes”, *The Guardian* (April 30, 2009).

<sup>13</sup> [www.coe.int/t/dgap/democracy/activities/key-texts/02\\_green\\_paper/Wish\\_list\\_en.asp](http://www.coe.int/t/dgap/democracy/activities/key-texts/02_green_paper/Wish_list_en.asp)

formation of a truly European information society.

I have so far illustrated the concept of e-democracy through the three points of Trechsel et al and more specifically through relevant examples for each of these points, but the doubt still remains as to whether or not e-Democracy can really work if put into practice. In relation to this Pratchett et al refer to Beetham<sup>14</sup> and observe that

...e-democracy adopts the Democratic Audit's criteria for democracy as having two fundamental principles that devices should be seeking to advance: political equality and popular control. Political equality refers to the principle that all citizens should have equal opportunities to influence decision makers in their locality. As well as offering mechanisms that theoretically support equality (e.g. universal franchise, one person one vote, etc); therefore, democracies should also include positive attempts to redress systematic imbalances in political engagement, develop inclusiveness and promote an equal sense of political efficacy among citizens. Popular control is the other side of the same coin and refers to the idea that citizens as a whole are able to control and direct what governments do on their behalf. Consequently, it includes such principles as transparency in government processes, accountability of governments and public servants, and responsiveness in policies and practices.<sup>15</sup>

Hence, if we take political equality and popular control and use them to gauge the effectiveness of e-democracy we can observe that, for instance, electronic voting can fulfil the requirements of the former. This is the case because electronic voting has indeed the potential of increasing the participation of socially excluded groups and of those who because of some physical handicap cannot reach the traditional voting booths. Similarly, democracy kiosks have the potential to develop inclusiveness among the citizens because these will allow the same citizens to interact with their

---

<sup>14</sup> David Beetham, "Theorising Democracy and Local Government" in D. King and S. Desmond (Eds), *Rethinking Local Democracy*, (Hampshire: Palgrave Macmillan, 1997).

<sup>15</sup> Lawrence Pratchett, "Barriers to e-Democracy: Local government experiences and responses" in Local e-Democracy National Project (May 27, 2005).

elected representatives. Hence through such mechanisms, citizens will possibly be in a position to be part of the political system on a continuous basis and not only once in every four or five years (that is when they are called to elect their representatives). If on the other hand we try to assess popular control, one can notice the potential that both parliamentary websites and television have in this regard. This is the case, because these tools can indeed increase both transparency and accountability in relation to governmental processes. Nevertheless, Pratchett et al do also warn that

The implications for e-democracy of these two simple concepts are significant. No democracy, at the level of either the nation state or local government, can claim to have met them fully. Citizens do not have equal power in their locality and governments are often accused of ignoring citizens' wishes. For democracy to work, therefore, it needs to have a number of mechanisms, all of which seek to achieve, in different ways, components of political equality and popular control. Furthermore, these mechanisms need to be continuously reviewed and updated to ensure that they remain relevant to the values that they are seeking to support.<sup>16</sup>

This advice is indeed very factual because it is certainly not sufficient to just proclaim the benefits of e-democracy and then not have the proper mechanisms which can practically support the declared benefits. For instance, as already mentioned regarding electronic voting, a lot needs to be done to make this secure enough for it to attract the citizens' confidence. On the other hand, it is not enough to have parliamentary websites if these are not updated on a continuous basis with new laws and proposed regulations. Moreover, if what governments want is real participation they should give the opportunity to citizens (through present-day information technologies) to submit their opinions on proposed laws which are still under discussion, rather than just posting the laws once they have been legislated. After all, the information society should be promulgating two-way communication rather than one-way imposition.

---

<sup>16</sup> Ibid.

#### IV. E-government

The second e-mechanism which requires our attention is that of e-government, a term which should not be confused with e-democracy although the two are related. Almarabeh and Abu Ali observe that

...there are multiple definitions of e-government among researchers and specialists, but most of them agreed to define electronic government as government use of information communication technologies to offer for citizens and businesses the opportunity to interact and conduct business with government by using different electronic media such as telephone, touch pad, fax, smart cards, self-service kiosks, e-mail, Internet, and EDI. It is about how government organizes itself: its administration, rules, regulations and frameworks set out to carry out service delivery and to co-ordinate, communicate and integrate processes within it.<sup>17</sup>

Hence, e-government is indeed more of a service (or a collection of services) rather than a mechanism per se. As a matter of fact, e-government is much more tangible than it has been so far the case with e-Democracy and this is the case because through e-government, citizens of the information society can among other things request documents and submit applications electronically rather than having to do it personally by visiting some governmental department or ministry. Hence, where this service is already available, citizens can for instance renew their national identity cards and/or passports online and thus avoid travelling and having to endure long queues. Indeed, this is just one example among many which one would typically find in an e-government framework. Other factual examples are the submission of online applications for trading licenses and applications for vacancies within government departments and ministries.

The so far mentioned examples do indeed demonstrate that a number of services which are offered within the information society are both

---

<sup>17</sup> Tamara Almarabeh and Amer Abu Ali, "A General Framework for E-government: Definition, Maturity Challenges, Opportunities, and Success" in *European Journal of Scientific Research*, Volume 39, Number 1 (2010), pp. 29-42.

positive and valuable, and that undeniably they can be of great help for the knowledgeable citizen. However, as Steven Clift rightly warns,

A significant barrier to e-government efforts that enhance online participation are bureaucratic fears of quantity over quality. The scarcity of time faced by citizens is a challenge for civil servants as well. Without structured ways to gather, evaluate, and respond to public input online, there will be diminishing value received or perceived with each additional public comment. Achieving greater consultation with value-added citizen input is the area of the most considerable e-government and democracy activity in the executive or administrative branch of government.<sup>18</sup>

Hence, Clift is here urging us not to fall into the trap of transforming one kind of bureaucracy (offline) into a new form of bureaucracy (online). It is indeed imperative that e-government streamlines traditional processes and not just give them an ineffectual facelift. As a matter of fact, if effective streamlining is not carried out, citizens will just be queuing in the informational superhighway rather than in the corridors of a governmental department!

Steven Clift also declares that “One indicator of e-government and democracy success will be the increased understanding online users gain about government. To effectively participate in your government you need access to the ground rules, including information on the proper way to make freedom of information requests that go beyond what governments share online at their discretion. Without these seemingly mundane information components in place, efforts to encourage deeper public participation will lack the necessary foundation.”<sup>19</sup> This is indeed a very eloquent observation and as a matter of fact that is why I have previously introduced Clift’s passages with the term “knowledgeable citizen”, because unless the citizen is conversant with both the conventional governmental processes and with information technologies, he will not be able to make effective use of e-government services. This is for instance confirmed by Choudrie and

---

<sup>18</sup> Steven Clift, “E-government and Democracy: Representation and Citizen Engagement in the Information Age” in *Publicus.Net* (February, 2004).

<sup>19</sup> *Ibid.*

Dwivedi who in relation to e-government services offered in the UK (which is undeniably one of the most advanced information societies that exist nowadays) observed that the majority of the adopters were between the age ranges of 25 and 54 years. Moreover they state that one interesting result was that the adoption rate declined considerably after 54 years and no respondents were reported at the 64-years plus category. Indeed, they believe that this is the case “because this age group consists of mostly non-computer users who do not possess the skills and knowledge necessary in order to use the computer and Internet”.<sup>20</sup> Hence, from this we can essentially observe how Choudrie and Dwivedi agree with Clift regarding the fact that unless citizens possess the necessary “foundation” they will not be able to benefit from the “goods” that the information society has to offer.

## **V. The Information Age and globalisation**

In our information age, all nation states are affected in some way or another by the processes of globalisation and many of these processes are initiated or take place in countries which are already information societies. Consequently, it is of utmost importance that globalisation is also discussed in relation to the main theme of this paper.

As a matter of fact, a recurring discussion within the theme of globalisation is the role of the nation state since as it has been argued in the beginning of this paper; nation states have to operate within a political and economical climate where their power is seen to be contested by the international flow of information and by MNCs. In relation to this, Christopher May writes that

Much of the debate and comment about the information age as it relates to states dovetails with claims made about globalization and its effects. But contemporary commentators have been remarkably myopic. In many cases only the state can offer the support that MNCs may find attractive (infrastructure provision, tax holidays and the protection of their property

---

<sup>20</sup> Choudrie and Dwivedi, “A Survey of Citizens’ Awareness and Adoption of e-government Initiatives, The Government Gateway: A United Kingdom Perspective”, paper submitted at the e-Government Workshop. Sept. 13, 2005.

rights).<sup>21</sup>

Here, May is referring to those commentators who believe that globalisation has rendered obsolete the idea of nation states. Indeed, May sees nation states as pivotal in the information age and although he is here referring to the nation state's role in relation to the MNCs I also contend that their role is also crucial in the free flow of information across national borders. My observation is supported by the fact that nation states are the ones who both initiate and oversee the construction of local grids which are necessary for the required flow of information. Moreover, the allocation of the required frequencies on which the transport of both local and international information takes place is also carried out by national governments. Hence, this also amply demonstrates how the role of each individual nation state is still important in the construction of a future information society which is aspiring to become truly globalised.

While notwithstanding the fact that the role of the nation state is still an important one, it is also true that in the information age, the processes of globalisation have influenced and shaped the roles of individual nation states and if we observe this within the context of the New International Division of Labour (NIDL) we will be able to see that it is not only those nations which have already become information societies that have been affected. In relation to this, Ietto-Gillies states that

...the interests and activities of TNCs led to new developments in the production process by which the product would be divided into several components according to the skills required. The components requiring low skills would be located in developing countries (often in export processing zones) and those requiring high skills would be located in developed countries ... A similar pattern is now developing for many services - or services components of goods - because of the new technologies. We could be talking of an electronic-age "new international division of labour" (e-NIDL) in which the ICTs allow increased scope for the conditions which led to the NIDL. In the e-NIDL the scope for

---

<sup>21</sup> C. May, *op cit.*

division of the manufactured products into appropriate components is still applicable. However, to this we must now add the scope for division of services into components some of which can be transmitted electronically for further processing in other locations.<sup>22</sup>

The above observation by Ietto-Gillies is indeed a credible one because it is the case that MNCs are now making full use of information and communication technologies to allocate the various work which pertains to the processing of information in different countries. All of this can be easily observed across various information-based industries. If for instance we take the computer software industry which nowadays generates billions of revenues worldwide, we can observe how the multinational software companies are splitting their operations across the countries in which they own local offices. For instance a company with its headquarters in the USA might keep its research and development together with its marketing and sales divisions in the most affluent information societies, while it outsources the development of software to Ukraine which has a lot of talented and lowly paid software programmers. This is something which its occurrence can be confirmed by Andrea Curti of the *Kyiv Post* who wrote the following: “Where does a Western businessman go when he needs state-of-the-art software tailored to his business? Instead of drawing expertise from their expensive domestic labour market, many Western firms are now looking east, taking advantage of the highly skilled and inexpensive labour force here in Ukraine and other parts of Central and Eastern Europe, including Russia”.<sup>23</sup> After-sales support is then usually provided by countries such as India and accordingly telephone calls of customers who need help with using the software programs are redirected through digital exchanges located in the affluent information societies to the myriad of call

---

<sup>22</sup> Grazia Ietto-Gillies, “Internationalization and the demarcation between services and manufacturers: a theoretical and empirical analysis” in M. Miozzo (Ed), *Internationalization, Technology and Services* (Camberley and Northampton: Edward Elgar Publishing Limited, 2003).

<sup>23</sup> Western Firms turn to Ukraine for Programmers. [www.auriga.com/en/press-room/articles/detail.php?ID=782](http://www.auriga.com/en/press-room/articles/detail.php?ID=782)

centres that have been setup by the multinational corporations in the western-friendly developing nations.

All of the above is certainly of benefit, primarily for MNCs and to a lesser extent also for governments of developing nations, because the former are seen by the latter as generating the much needed work places. Nevertheless, this whole scenario is also creating a lot of uncertainty among most workers in both established information societies and in those which are aspiring to become so. This is confirmed by Pintér who in reference to Castells states that

Information and communication technology provides the infrastructural background which is financially supported by the new heavily globalised network economy. A predictable consequence of this transformation process is the growth of social insecurity, a weakened capacity for prediction and plan-making, as well as the appearance of new social inequalities that create a fourth world of outcasts. Networking is the new logic, the new organizing principle of society. The rule is simple: those belonging to the network exist, while the network outcasts are non-existent. Since humanity is basically a self-centred entity, with its identity defined by one particular location and culture this process generates immense tension. Individual workers and the human labour force, in general, cannot pursue the constant wandering of capital and hence, job opportunities, on a global level.<sup>24</sup>

Hence, as Pintér rightly observes, the processes of globalisation are creating social insecurity because workers in the affluent information societies are under constant threat of having their jobs outsourced to workers in developing countries, and on their side workers in the developing nations know that if they demand wages and work conditions which are similar to those of their western counterparts they might see their jobs transferred somewhere else. Moreover, it is also the case that such global

---

<sup>24</sup> Róbert Pintér, "Towards getting to know information society", *Information society - From Theory to Political Practice* (Budapest: BPR Publishers 2008).

arrangements have created a number of disparities in both the developed and the developing nations. This is the case because those who are not considered to be connected knowledge workers cannot be in a position to integrate in the electronic-age equivalent of the New International Division of Labour.

Moreover the level of generated insecurity is not only related to labour, but as Pintér observes,

The growth of tension is also reflected in social movements. Some of these (religious fundamentalists, for instance, among other reactive movements) withdraw into traditions and religious values regarding stability, and lack of change as something precious. Others, (anti-globalisation proactive groups) turn against the network society, ironically enough, exploiting the latter's own means of globalised technology and culture. Global criminal economy presents another difficulty that societies have to face, and to make things even worse, in certain countries such crime is entangled with the legal political power. This circumstance in the end is something that poses a threat to the entire globalised world. The workings of the globalised information society eventually have its impact on everyone. However, not every individual participates in the construction of the new mode of living, in the same way as not all of us become part of the network.<sup>25</sup>

Hence, from Pintér's passage we can observe how ironically the processes of globalisation can sometimes have the opposite effect, like for instance that of creating antagonising localised realities. This happens in response to the effects of the same globalising processes which are sometimes seen as being too invasive vis-à-vis local culture and tradition. Another problem also arises through the new forms of criminality because many criminal organisations have embraced globalised information and communication technologies to create criminal networks which extend beyond traditional boundaries. These and other globalised realities are

---

<sup>25</sup> Ibid.

certainly already creating far-reaching effects on the whole of humanity.

## **VI. Privacy versus surveillance in the information society**

One of the indistinguishable features that one cannot fail to observe in the Orwellian world of the novel *Nineteen Eighty-Four* is mass surveillance. As a matter of fact, in 1949, Orwell had imagined a future world where humanity could be easily observed through the use of ubiquitous technology. Since Orwell published his book, more than sixty years have passed and people living in the information society can be observed through cameras that are found in shopping malls, in the streets, at airports and sometimes even at home through interactive television and web cameras. Also, whereas in *Nineteen Eighty-Four* people were aware of mass surveillance, in many instances the citizens of the information society are not aware that they are being observed. At the same time, the promoters of the information society do also advocate an Athenian world where personal privacy is considered to be of utmost importance. So, in the information society which of these two opposing features is the one which really prevails?

In the information society surveillance can be exercised through various mechanisms. For instance Pintér observes that “The life of the citizen as a consumer can be tracked, without doubt, through an increasing level of precision by a sophisticated range of information technologies”.<sup>26</sup> The information technologies which track consumer behaviour are numerous. For example through Pay-Per-View programs on television, service providers are able to build up profiles of what type of programs each subscriber is watching the most. This profile can then be used to target each subscriber with individualised marketing. For instance if a profile of a particular subscriber shows that he is mostly watching the football games of a particular team, then that subscriber can be targeted via sales campaigns which aim to sell merchandise related to that particular football team. Similar mechanisms can also be used on the World Wide Web via tracking “cookies” which are small text-files that are stored on a user’s computer while browsing websites.

On July 5, 1993, *The New Yorker* published a cartoon depicting two dogs in front of a computer with a caption stating “On the Internet, nobody

---

<sup>26</sup> Ibid.

knows you're a dog". This referred to the then common but erroneous assumption that on the Internet one could hide or not disclose his real identity. But in reality, there are various ways and means in relation to how identities can indeed be revealed. This is confirmed by Hosein who remarked that "The disclosure of user identities is increasing. A number of cases have emerged worldwide where courts have ordered the disclosure of the identities of internet-posters, e-mailers, and mere users. Copyright rules that require the release of subscriber information of suspected file sharers only makes matters worse for the protection of personal privacy".<sup>27</sup> Indeed, Internet service providers store usage logs for every subscriber and through a technical analysis of these logs any competent authority can know which websites were visited at any point in time and by whom. Most Internet users are not aware of this, and moreover only the minority possess the required technical knowledge to circumvent such surveillance. Hosein also observes:

Using the argument that the retention of traffic data was critical for the war on terror, a number of countries adopted retention policies. In December 2001 data retention was introduced and passed under the United Kingdom's anti-terrorism law, followed by France and many others in the EU, with other countries following quickly including South Africa, and Argentina. All these countries now require ISPs (and telephone companies) to keep the traffic data generated by their customers for lengthy periods of time in case the data may be of value for an investigation of any crime.<sup>28</sup>

Hence, in all of these information societies, any kind of electronic communication that takes place between citizens is being recorded and stored for a number of years with the proviso that only legally established authorities can access it. However, what these authorities usually fail to mention is the fact that both ISPs and telephone companies are manned by technically knowledgeable human beings who can at any time "look into"

---

<sup>27</sup> Gus Hosein, *Politics of the Information Society: The Bordering and Restraining of Global Data Flows*, (Paris: UNESCO, 2004).

<sup>28</sup> Ibid.

the stored communication that concerns other human beings. Moreover, the stored communication can also be accessed by highly knowledgeable unauthorised users if these manage to remotely retrieve the same communication by hacking into the ISPs' or telephone companies' digital networks.

As Hosein rightly claims, "These new policies permit the mass surveillance of individuals, and enable the sharing of this personal information across borders..." and adds that "The general public appear relatively unaware of these regimes for mass surveillance".<sup>29</sup> Indeed, the only times that the general public is made aware of such surveillance policies is when the contract which binds a subscriber to an ISP or a telephone company is initially signed and when the media publishes an article or broadcasts a piece of news which are related to such directives. However, as regards the former the "information" which should in theory make the subscribers aware of the surveillance is printed using small characters and written using legal terms. As a consequence only a few subscribers bother to read it. On the other hand, even though some media try to inform their readers or viewers of such directives, this only happens in rare occasions and usually it is only the minority that bothers to reflect on the possible consequences!

From what has been so far depicted the situation does indeed not look very rosy and most evidence seems to show that the information society, at least in relation to citizens' privacy is quite similar to an Orwellian type of society. However, Pintér contends that

Whereas the state attains increasingly efficient means of surveillance, citizens can gain easy access to information that they can employ against any transparent and controllable state mechanism. There is a gradual expansion of the individual's freedom that runs parallel with the rising transparency of the state. This implies that both sides by fulfilling opposing interests can utilize the new processes. It is not only the state that gains further resources but citizens too.<sup>30</sup>

---

<sup>29</sup> Ibid.

<sup>30</sup> R. Pintér, *op. cit.*

Hence, according to Pintér the whole issue which puts privacy against surveillance is what in game-theory would be described as a win-win situation, and that consequently all parties can benefit from it. While I do agree that his argument has a degree of merit, it is also a fact that not everyone is in a position or has the right knowledge to gain easy access to information. Consequently, it can indeed prove difficult (if not impossible) for these citizens to gain easy access to information that they can utilise against any apparent state mechanism! Hence, for such citizens it is usually the state and commercial corporations who have the upper-hand in relation to mass surveillance over citizens' privacy.

Indeed, it seems that also Pintér is aware of potential issues that may exist in relation to privacy and surveillance but in this regard he states that "Even if mass surveillance arises as a significant problem, our evaluation of present democracies indicates there are inbuilt guarantees in democracy for the management of such centuries old difficulties with the misuse of power. These past guarantees may need revision in order to accommodate the altered circumstances thus preserving their efficiency and recognition".<sup>31</sup> It seems to me that in this regard Pintér is over confident as regards the possibility of guarantees which ought to prevent the misuse of surveillance because until governments and private corporations are in a position to be in control of the medium, it will be very difficult for the majority of the citizens to find effective ways on how to even detect any misuse of power. Indeed, most information-age citizens find usually themselves in situations where they either accept all imposed conditions or else they are totally barred from gaining access to information!

## **VII. Where does power lie in the information society?**

All of the social entities that I have discussed throughout this paper are very relevant within the context of the information society but nevertheless it is still not clear who out of these discussed social players holds the power. The only author who has specifically elaborated on this is Manuel Castells and although in his treatise he constantly refers to the Network Society, it must be noted that the latter term is equivalent to the notion of the information society.

---

<sup>31</sup> Ibid.

Castells observes that those who have an interest in acquiring power seek to create social networks which can include various players. More specifically he states that “Social actors may establish their power position by constituting a network that accumulates valuable resources and then by exercising their gate keeping strategies to bar access to those who do not add value to the network or jeopardize the interests that are dominant in the network’s programs”.<sup>32</sup> Central to these social networks are their programs, which are the set of objectives that each network aims to reach. For instance one of the programs of a particular network could be that of becoming the major media empire in a particular region. In this regard it is essential for those who are part of the network to make sure that the objectives are both reached and maintained, and any group who cannot contribute towards reaching the network’s objectives will be barred from joining the same network.

Castells also observes that “power is exercised not by exclusion from the networks, but by the imposition of the rules of inclusion... Network power is the power of the standards of the network over its components, although this network power ultimately favours the interests of a specific set of social actors at the source of network formation and of the establishment of the standards.”<sup>33</sup> and as a specific example he mentions the so-called Washington Consensus as the operating principle of the global market economy which he identifies as a power network<sup>34</sup> The latter refers to a set of objectives which between 1980 and 2008 pushed forward the idea of a globalised free-market economy. This network power included various social actors such as influential politicians, free-market economists, popular journalists and global organisations such as the World Bank and the IMF. Hence in this case, anyone who wanted to be part of this power network had to adhere to the objective of pushing ahead with a free-market economy and all those social actors who were opposed to such objective were automatically excluded.

Castells is also very specific in relation to the amount of power that each social actor within a power network has. For instance he observes that

As for the capitalist class, it does have some power, but not

---

<sup>32</sup> Manuel Castells, *Communication Power* (Oxford: Oxford University Press, 2009).

<sup>33</sup> Ibid.

<sup>34</sup> Ibid.

power over everyone or something: it is highly dependent on both the autonomous dynamics of global markets and on the decisions of governments in terms of regulations and policies. Finally, governments themselves are connected in complex networks of imperfect global governance, conditioned by the pressures of business and interests groups, obliged to negotiate with the media which translate government actions for their citizenries, and periodically assailed by social movements and expressions of resistance that do not recede easily to the back rooms at the end of history.<sup>35</sup>

Hence, according to Castells none of these social actors (the capitalist class, governments, regional groupings, NGOs, the media and social movements) hold ultimate power over the others. Rather, power is shared between all of them and is kept in balance by the reciprocal relationships that each of them have within the network. Consequently, any local government who is at the helm of a networked information society, cannot hold absolute power but the latter has to be shared with the other partners within the network.

### **VIII. Conclusion**

Throughout this paper I have illustrated the main developments that have been taking place over the past couple of decades in the most economically advanced nation states. It is my hope that at the end of my interpretation the attentive readers will be in a better position to appreciate the fact that the new forms of governance which are present in our “Information Age” have the real potential of offering a number of benefits to the citizens of information societies. Nevertheless, I do also believe that at this stage most of the tools and mechanisms which are required to make these new forms of governance effective are still in their infancy. As a consequence, none of these tools and mechanisms has managed to gain widespread support and for this to be one day possible the underlying technologies need to both improve and also become more available.

Throughout this paper I have also amply demonstrated that as consequence of the use of information technologies and also as a consequence of the processes of globalisation, nation states have to endure a

---

<sup>35</sup> Ibid.

number of drastic changes in relation to how they control their subjects. Indeed, most nation states have no other option other than to share their power with a number of local, regional and global social actors and together with these they actively participate within a number of informational power networks. At the same time, there are still a few nation states which aggressively persist in not sharing their power with others and as a consequence of this they are being excluded from being part of the informational power networks.

It must also be noted that all governments of those nation states which have decided to embrace the information revolution, are still trying to put certain restrictions in relation to their citizens' privacy rights and in this regard mass surveillance can be easily carried out through the use of information technologies.

Finally, I will end this paper by reminding all readers that the information society is still evolving. Consequently, in the years to come, all that I have discussed will need to be re-examined on a continuous basis, and in this regard I indeed believe that this is one of the main missions that philosophy has to undertake in the 21st century.