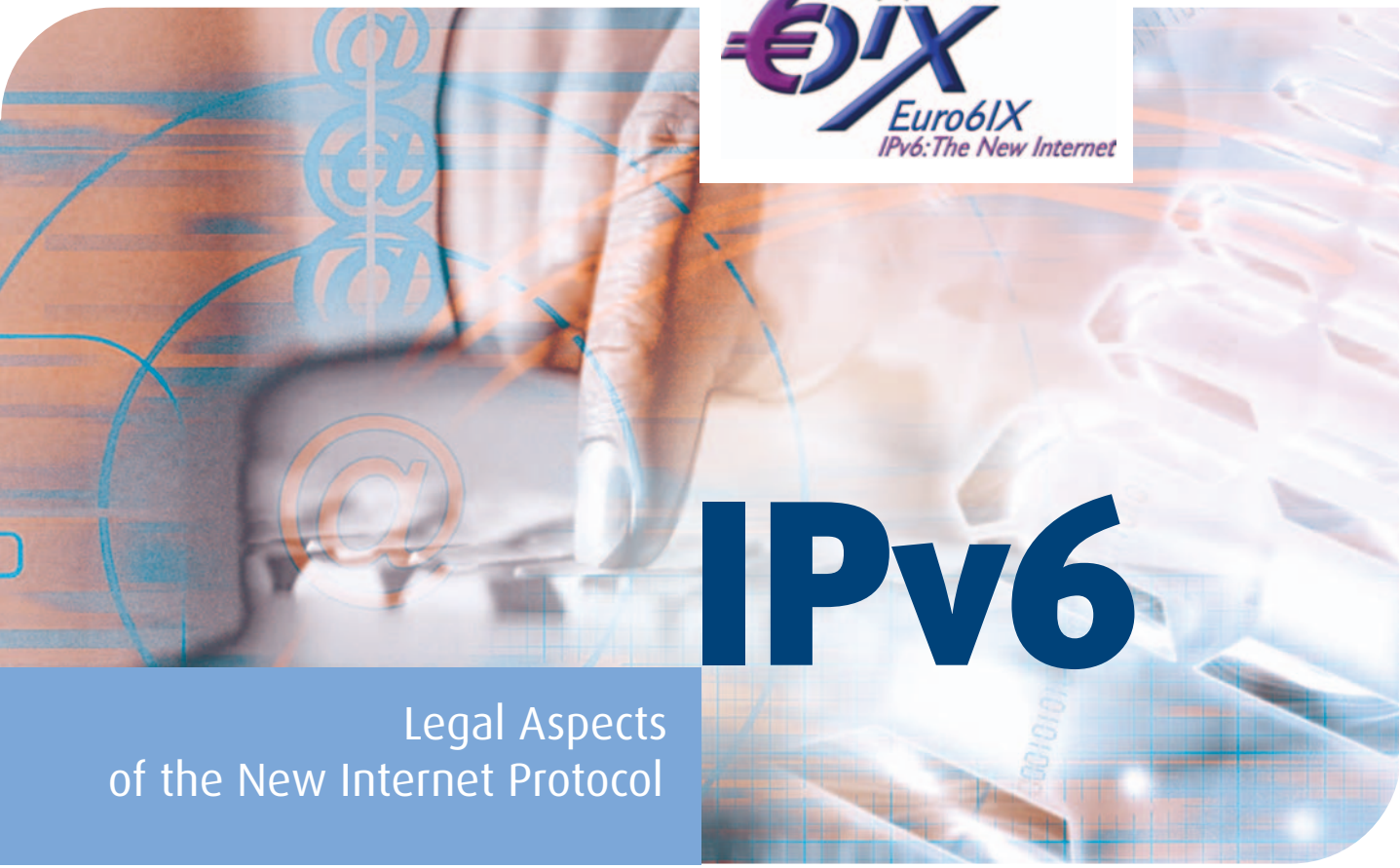
A reference book regarding the main legal aspects related to the deployment and use of IPv6



IPv6

Legal Aspects of the New Internet Protocol

Aspectos Legales del Nuevo Protocolo de Internet

ConsulinTel
Consultores Integrales en Telecomunicaciones

ECIJA

Manual de referencia sobre los principales aspectos legales relativos al despliegue y utilización de IPv6

Legal Aspects of the New Internet Protocol

A reference book regarding the main legal aspects related to the deployment and use of IPv6

Aspectos Legales del Nuevo Protocolo de Internet

Manual de referencia sobre los principales aspectos legales relativos al despliegue y utilización de IPv6

Euro6IX
IPv6:The New Internet

IPv6: Legal Aspects of the new Internet Protocol

ISBN 84-609-6359-4

Edited by Euro6IX with the support of the European Commission.

This book was made possible thanks to the cooperation and contributions of Euro6IX project participants and David G Mills (Southampton University).

If you have any questions or comments or you would like to receive another copy of this book, please visit *http://www.ipv6tf.org*

On-line PDF version also available *(http://www.ipv6tf.org/pdf/ipv6legalaspects.pdf).*

IPv6: Aspectos Legales del nuevo protocolo de Internet

ISBN 84-609-6359-4

Editado por Euro6IX con el soporte de la Comisión Europea.

Este libro ha sido posible gracias a la cooperación y contribuciones de los participantes del proyecto Euro6IX y David G Mills (Universidad de Southampton).

Si usted tiene alguna pregunta o comentarios o desea recibir copias adiccionales de esta publicación, por favor visite *http://www.ipv6tf.org*

Se hayan disponibles versiones on-line en formato PDF *(http://www.ipv6tf.org/pdf/ipv6legalaspects.pdf).*

Introduction

- What is IPv6, the new Internet Protocol?
  Main aspects and characteristics
- Deployment of IPv6: current situation and experiences
- Implications of its deployment
- Legal consequences:
  - How could IPv6 affect the right to privacy of the users?
  - Could an IP address be considered as personal data?
  - How could IPv6 help to fight against piracy?

- **What is the target audience?**

  In house lawyers
  Security Managers
  Lawyers
  Consultants
  Technology Manufacturers
  Internal Audit Managers
  Executive Directors
  Telco´s
  ISP´s
  Web Pages
  Organization Managers

IPv6

Legal Aspects

contents

table of contents

table of contents

table of contents

table of contents

three

table of contents

four

table of contents

Prologue

The extraordinary growth of new technologies and, specifically, the future implementation of the IP Protocol in version 6 (IPv6) opens an enormous variety of possibilities, activities and new ways to communicate, work, buy, establish new means of relationships with other people and, therefore, to carry out most of the activities of our daily life.

For example, the possibility of locating the exact place where a certain mobile device is, to have a refrigerator able to connect itself to the supermarket and order the products needed or to be able to decide which addresses are authorized to receive a song downloaded through the Internet, are examples of situations where IPv6 becomes an almost essential element that helps, among others factors, these activities to become a reality.

In this sense, IPv6 receives special relevance in this matter since version 4 of protocol IP (IPv4), at present, has some limitations which prevent a better development of these new advances and their effective operation. Such limitations include, for example, technical specifications that do not allow easily its extension, the limited number of available IP addresses, etc.

For that reason, although the main objective of these new technological advances based on IPv6 is to improve the quality of life of their users, they also primarily aim to carry out important works of development and technological investigation that require an international implication.

Secondly, it is necessary to consider legal implications that the implantation of IPv6 entails, in order to assure that its use is carried out in accordance with the applicable legislation and that its implementation does not harm this legislation nor the rights and liberties deemed for its users.

The concern about legal implications that IPv6 could have was shown in the Opinion 2/2002 relative to the use of unique identifiers: The example of IPv6, 30 of May, of the Article 29 Working Party.

In particular, their apprehension was based on the existence of 'Unique Identifiers' in certain types of IPv6 addresses. These identifiers are able to leave signs as a 'track', for example, in those cases when a person access a web page, it could be possible to obtain a detailed study of his profile, preferences, etc, and to track all the activities he is doing through the Net.

Questions began to surface, like 'What legal consequences can exist?', 'Would the privacy of the users be affected with IPv6?', 'Are there any implications on data protection?', 'What could be done with the obtained information regarding the surfing habits of a user?' etc, therefore, a clear answer is required.

Prologue

Nevertheless, although these doubts were related to different issues, the main preoccupation was centred in the existence of possible infringements that IPv6 could entail with respect to the right to privacy.

Also some doubts arose about the legal consequences of the consideration of an IP address as personal data.

Soon, some initiatives were fostered that began to address these legal questions, since it became a general conviction that the good development of IPv6 was directly linked to the confidence of this Protocol that the users deemed. In this sense, it was agreed that it was necessary to acknowledge not only its technical implications (what it is; how it works, what are the advantages of its use; what does its use entail, etc) but the legal aspects as well (its legality; possible rights infringements; obligations of IPv6 providers, etc).

Within the initiatives commencing as a result of the investigation, architectural design and deployment of IPv6, the Euro6IX (European IPv6 Internet Exchanges Backbone) Project was born. Its main task was, on one hand, to promote the investigative activities on this new version and, on the other hand, to make possible its rapid implementation throughout Europe.

Among all the people that formed part of the Euro6IX Project, the clear priority of requiring a legal study on this Protocol was concurred and, therefore, this study was carried out on the matter of privacy, data protection and intellectual property rights (copyrights). In this sense, some parts of this book contain the results of these studies prepared during the above mentioned Project.

This book aims to contribute some basic knowledge about the technical specifications of IPv6 (what is IPv6, how it operates and the current worldwide situation of its implementation). It also aspires to analyse, from a legal point of view, the problems and possible solutions that could exist regarding the following scopes:

- Right to privacy
- Data Protection
- Intellectual Property Rights (copyrights)

These legal considerations will not only be observed in relation to the infrastructures and networks developing activities, but they will be taken into account regarding the services provided through these infrastructures and networks, for example, VoIP services, interchange of files, instantaneous mail, access to audio-visual contents, etc.

Prologue

Once these legal problems derived from IPv6 are analysed, this book will propose some possible solutions of diverse nature: technical solutions included in IPv6; new legislative changes in order to regularize these problems or, in other occasions, searching for feasible ways to fulfil the existing legal obligations.

In this sense, acquiring knowledge about IPv6, its functionalities, advantages and disadvantages as well as the existing technical and legal solutions constitutes the first step in order to help its successful deployment.

Hence, IPv6 already gathers the backing of important organizations that support its definitive deployment, for example, universities, technological companies, telecoms as well as important companies dedicated to mobile telephony. These companies understand that, since the number of mobile phones presently surpasses the number of fixed telephones, IPv6 becomes the unique architecture able to support this number of mobile phones that can be connected to Internet and the services demanded by the users of this type of telephony.

In addition, at the present time, most of the service providers in research and big commercial networks, already provide IPv6 services.

All these initiatives show that IPv6 is not viewed so much as a project, but is being considered as a reality that is affecting all the spheres of daily life, improving the capacity of communications between its users and moving forward to the New Era of Internet.

1. The IPv6 Protocol

1.1. What is IPv6?

IPv6 is an upgrade to the Internet Protocol, which is central to the working of the Internet. The Internet Engineering Task Force (IETF) developed the basic specifications of IPv6 during the 1990s after a competitive design phase used to select the best overall solution. The primary motivation for the design and deployment of IPv6 is to expand the available address space of the Internet, thereby enabling internetworking of billions of new devices (PDAs, cellular phones, appliances, etc.) and new users (countries such as China, India, etc.). Broadband for all and 'always-on' technologies, such as xDSL, cable, Ethernet-to-the-home, fibre-to-the-home, Power Line Communications (PLC), etc., are a key driver for the demand of IPv6.

While the existing protocol, IPv4, has a 32-bit address space that provides for a theoretical 2^{32} (approximately 4 billion) unique globally addressable hosts, in practice, the number of global IPv4 addresses that can be used is far less, due to inefficiencies in address allocation and use. IPv4 has inherently a limited addressing capacity to provide for Internet scaling and potential to enable billions of devices to be globally connected where appropriate. Network Address Translation (NAT) has extended IPv4's life in conjunction with private IPv4 addresses. However, NAT adds complexity to the deployment of new end to end models inhibiting Internet growth and innovation including 'always-on' and 'peer-to-peer' services that require secure and constant access to devices for instance in home networks. IPv6 is here to ease out these two issues by providing a virtually unlimited address capacity that can uniquely address 2^{128} (about 340 undecillion(1)) hosts.

IPv6 plays a fundamental role in the deployment of 3G cellular networks, together with new multimedia services and applications, and its importance has been recognized by the European Commission and the European Council, back in early 2002 alongside broadband and 3G. Consequently, the *e*Europe 2005 action plan on '*the widespread availability and use of broadband networks throughout the Union by 2005 and the development of Internet protocol IPv6.... and the security of networks and information, eGovernment, eLearning, eHealth and eBusiness*'.

Today, IPv6, 3G and broadband (including PLC) are already starting to take off, and a new plethora of services and applications will soon no longer just be a dream. These technologies enable the Ambient Intelligence vision, with smart scenarios, which may start with digital IPv6-enabled homes, *e*Safety in vehicles, and better network operation and management to allow the ISPs to offer all the related services.

(1) Actually 340, 282, 366, 920, 938, 463, 463, 374, 607, 431, 768, 211, 456 addresses

1.2. Main differences between IPv6 and IPv4

As indicated above, IPv6 was initially designed with a compelling reason in mind: The need for more addresses.

Of course, there may be alternative technical solutions, such as NAT (Network Address Translation), but they won't work as easily to allow growth, new enhanced applications and services, and in general the new innovation taking place. Furthermore, those techniques make the Internet, the applications and even the devices more complex and this means a cost increase, while IPv6 can make, in the medium/long-term, every IP device cheaper, more powerful, and even consume less power (which is not only important for ecologic conservation, but also to have longer battery life in portable devices, such as cell phones).

Just to understand, in a non-technical way, what NAT is, lets use an example. Suppose that two people which can speak the same idiom, for example, English, need to use a communication channel which does not allow the usa of English. Then they need to use translators next to each of the speakers, on each side of the communication channel. It is obvious that some details of the communication could be lost with the translations. This is what happens today with the deployment of NAT in IPv4 internet: The lack of end-to-end communication disables the capabilities for services and applications to take complete advantage of the network, making it much more complicated and costly for management.

It is also true that NAT has been key for the Internet penetration in our daily life, due to the lack of enough public IPv4 addresses and while IPv6 was still reaching maturity. Today this is no longer the case, and NAT can now be considered as a kind of evil preventing innovation.

Consequently the design of IPv6 was an opportunistic way to improve the Internet, with new benefits, in addition to the expanded addressing capabilities. These include:

- Server-less autoconfiguration ("plug-n-play") and reconfiguration. With this feature the Internet becomes simpler, in the sense that is easier to automatically connect any device to the network. There is no reason to ask the users to configure the devices anymore, specially considering that new devices will not be just PCs with a screen and keyboard, but white goods, appliances, sensors, etc., that don't have this type of interface to allow configuration. In IPv4 this can't be done unless a server (for the DHCP protocol) is installed on the network, which means a higher cost for the server itself and for its maintenance.
- More efficient and robust mobility mechanisms. IPv6 has been designed under the perspective of a new nomadic world. Users and devices tend to move more than ever. The connectivity is important even when moving in order to provide enhanced services, especially in wireless environments. IPv4 also supports mobility, but is very inefficient compared with mobility in IPv6.

- End-to-end security, with built-in, strong IP-layer encryption and authentication. IPsec is the security protocol, the same as in IPv4. The main difference is that IPv4 doesn't mandate the support for IPsec, which means that it´s not always is available. Furthermore, in IPv4, because of NATs it is often not possible to use IPsec end-to-end, unless you have the knowledge to configure a tunnel or VPN among the two end stations and traverse the NAT. This is described further later on, in this chapter.
- Streamlined header format and flow identification. IPv6 protocol designers took advantage of the knowledge gained from the IPv4 usage expertise during the last years in order to improve the way the data is encoded to form the IPv6 protocol header, and consequently enhance the operation of the network. At the same time that the header was being simplified new functionalities were added one being the flow identification header, which will allow in the future a better operation of quality of service (QoS) mechanisms within the Internet in the future.
- Enhanced support for multicast. IPv6 includes an enhanced support for multicasting, as well as an embedded feature of the protocol, which is key for the usage of broadband networks for multimedia contents distribution.
- Extensibility: Improved support for options / extensions. Last, but not least, IPv6 has been designed with the ability to grow in mind. In a few years time we don´t want to discover that we are in the same situation as with IPv4 with the design IPv6 being such that we handicap the extension of the Internet. IPv6 was designed to provide a means to incorporate new features in a flexible and unlimited way. We are able to incorporate new pieces to the protocol (the so called extension headers), without requiring the upgrade of all the devices on the network. Only those devices using the new extensions need to be updated, the same way that all the operating systems and applications get upgraded from time to time, in an automatic way, transparent to the user.

1.3. The Transition to IPv6

A very important aspect, since the earlier stages of the design of IPv6, has been recognizing that IPv4 will be coexisting in the network for a long time. This is due to the fact that there are already millions of devices, applications and services, which can't be disconnected even for a moment. Internet has become a critical infrastructure, and there is no way we can stop it, for example, even just for a single night, to upgrade it and get IPv6 working everywhere. It is also easy to understand that even if we could do that, there will be devices which can't be upgraded to support IPv6, for example because the manufacturer no longer exists, and most probably will not provide access to the code inside the device to upgrade it ourselves.

For this reason, IPv6 has been designed along a set of transition mechanisms, which allow the coexistence of both protocols, IPv4 and IPv6, for a long time, which will depend on a number of factors, scenarios, business sectors, etc. Moreover, those transitions mechanisms facilitate the integration of IPv6 in the existing IPv4 Internet.

Technically speaking we can say that IPv6 is mature: Today is possible to do with IPv6 all what we can do with IPv4 and much more. The clearly we can foresee a bigger development of new services and applications thanks to the deployment of IPv6. IPv6 will bring back innovation to Internet, which was killed with the deployment of NAT with IPv4.

A couple of years ago most of the networks supported only IPv4 and very few networks supported IPv6. Today the situation has radically changed and more and more commercial networks support IPv6. In the near future, we will see the entire Internet supporting IPv6 and IPv4 and we may even reach the point where some of the networks no longer support IPv4. Of course, end-to-end communication with IPv4 will always be possible, because we will still use transition mechanisms, but the other way around to how we use it today.

Is also remarkable that most of the research and education networks in the world already support IPv6 for more a year now. Several private and public institutions are heavily engaged in fostering IPv6 deployment, including the European Commission, the US Department of Defense, etc. For further information on the deployment status and worldwide support towards IPv6, refer to the IPv6 Cluster publications 'Moving to IPv6 in Europe'(2) and 'IPv6 and Broadband'(3). Updated status and information of the worldwide deployment situation is always available at The IPv6 Portal(4).

1.4. European IPv6 R&D Activities

The European Commission Information Society Technologies Program has funded a number of projects with a very important focus on IPv6 research and development activities. These projects represented a huge investment on behalf of the EC (over € 90M) and the project partners.

These projects can be divided into 2 groups. The projects of the first group, referred to as IPv6 Projects, have a particular emphasis on IPv6, with the main goal being the research and development related to the protocol itself. Projects of the second group, referred to as IPv6 Related Projects, are employing IPv6 as part of their broader goals.

The projects are addressing several complementary areas. Two large very scale experimentation platforms are investigating the real deployment of IPv6, Euro6IX being one of them. Some other projects are devoted to the promotion of IPv6. The political dimension is also addressed and a large set of projects are addressing different technical aspects related to IPv6 (e.g. IPv4 to IPv6 transition, Quality of Service, etc...).

(2) http://www.ipv6tf.org/news/newsroom.php?id=169 | (3) http://www.ipv6tf.org/news/newsroom.php?id=988 | (4) http://www.ipv6tf.org

The IPv6 projects as well as the IPv6 related projects have been collaborating in the frame of the IPv6 Cluster since June 2001. A specific project, 6LINK, is supporting the activity of the IPv6 Cluster.

2. The Euro6IX Project (European IPv6 Internet Exchanges Backbone)

2.1. What is the Euro6IX Project?

Euro6IX is the larger research project up to now funded by the European IST Program. The goal of the Euro6IX project is to support the rapid introduction of IPv6 in Europe. Towards this target, the project has defined a work plan. This describes the Pan-European network design (native IPv6), network deployment, research on advanced network services, development of applications (validated through the involvement of user groups and international trials), and active dissemination activities, including events and conferences, contributions to standards and policy (IETF and RIPE among others), publication of papers and active promotion of all the publicly available project results through the project web site.

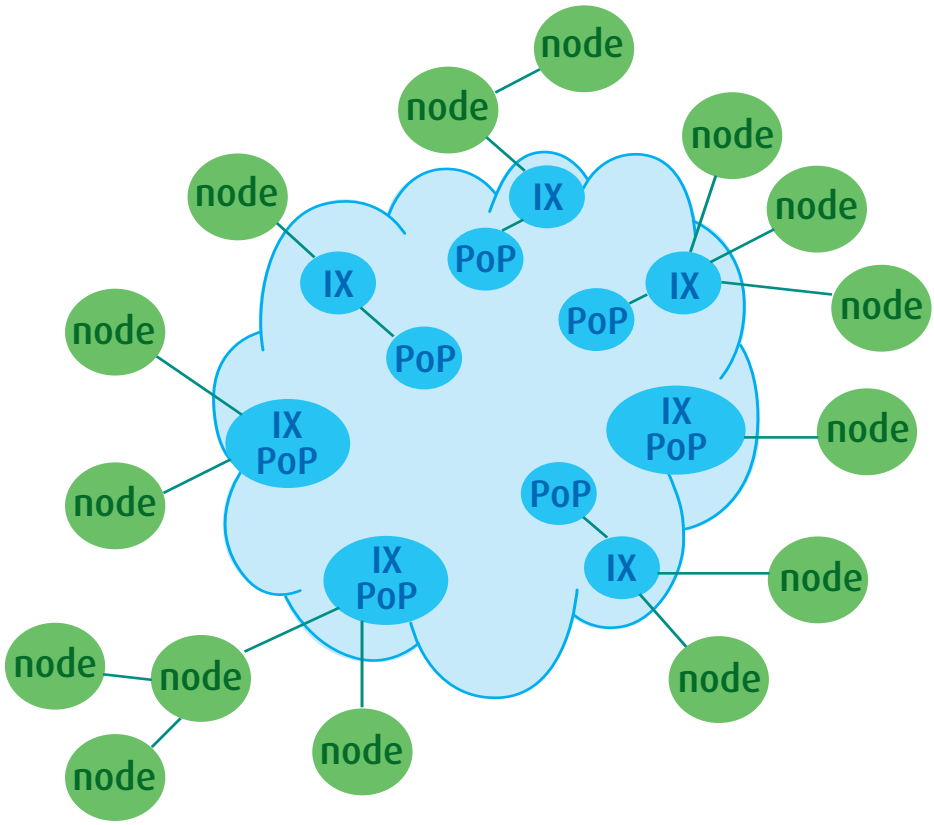
Euro6IX, started in January 2002, building dedicated, native, IPv6 networks, involving National Research and Education Networks, telcos and ISPs, in a complementary approach, and considering other aspects like applications, Internet Exchanges and legal aspects.

The project researched, designed and deployed a native Pan-European IPv6 network, called the Euro6IX test-bed. It included the most advanced services obtainable from present technology and followed the architecture of the current Internet (based on IPv4). It considered all the levels needed for the worldwide deployment of the next generation Internet. The infrastructure of Euro6IX consisted of the following different network levels:

- **IX-level:** Regional native IPv6 exchanges.
- **Backbone-level:** Pan-European core network that interconnects the regional exchanges and creates the highest level in the network hierarchy.
- **Node-level:** Service providers, ISPs and other providers accessing the core network to provide IPv6 services and end user access. The users will be connected by means of a variety of access technologies, including legacy IPv4 networks and services whenever no IPv6 native links are available or feasible. This level includes a set of academic, research and non-commercial trial users who will use native IPv6 services and generate IPv6 native traffic.

Preliminary Issues

A high **abstract level scheme** of the Euro6IX test-bed concept is pictured as follows.



Abstract Scheme of Euro6IX Test-bed

Euro6IX offered advanced network services, and a repository of IPv6 enabled applications, which have been ported, adapted or enhanced, and made available for trials both within Euro6IX and to third parties.

The native IPv6 traffic has been the result of both specific and generic applications tuned for IPv6 (e.g., IPv6 enabled Web browsers).

The validation has been performed in a realistic context where the different actors and roles, which exist in the present Internet, are extrapolated to the IPv6 based next generation Internet. This validation has been made through the involvement of existing and new user groups created by the project with the daily use of the network by project partners and through both, internal and public trials and other events.

Additional dissemination, liaison and coordination activities have been performed in clusters, standards organizations and with interested third parties in order to give to the results of the project the highest visibility and to achieve the largest impact.

The success of the Euro6IX project has been measured against the achievement of:

- Provision of efficient interconnectivity and advanced network services, for the complete IPv6 European level Internet.
- Involvement of research entities and non-commercial trial users (user groups) in order to validate the network, advanced services and applications.
- Promotion of the IPv6 interests by ISPs and users, standardization bodies and other related projects.

2.2. Goals pursued

The first objective of the Euro6IX project has been to research an appropriate architecture to design and deploy the first Pan-European non-commercial IPv6 Internet Exchange (IX) Network. It has connected several regional neutral IPv6 Internet Exchange points across Europe, and achieved the same level of robustness and service quality as currently offered by IPv4 Internet Exchange Networks. That is:

- To research and design a native IPv6 network which follows the hierarchical architecture of the global Internet by including:
  1. A set of regional native IPv6 Internet Exchanges;
  2. A core network to interconnect the exchanges;
  3. A second/access level of nodes, for ISPs, sites, corporations and users.
- To deploy the native IPv6 network based on the proposed architecture.
- To test, tune and improve the main protocols, algorithms and techniques needed to deploy and operate the network and the advanced services.

The involvement of the major/incumbent European Telcos in this project, covering also the bigger areas that have a higher Internet user growth rate, reflects the strategic importance of the fast and timely introduction of IPv6 in Europe.

The second objective has been to use the deployed IPv6 IX infrastructure to research, test and validate IPv6-based applications and services, such as:

- Investigations on the maturity of advanced IPv6 network services, as well as the feasibility of their inclusion in the Euro6IX test-bed, for example CoS/QoS, Mobility, Anycast and multicast, security, multihoming, renumbering, and policy languages.

- The development, porting, adaptation, or enhancement of IPv6 enabled applications, which have been made available for project trials and to third parties.
- The research of the legal implications of the project related to users, networks, and service providers addressing, personal data protection, and privacy concerns about IPv6 addressing.

As a **third objective**, the network built within the Euro6IX project has been open to specific user groups (existing and to be created), who will be connecting to the Euro6IX network by means of a variety of access technologies – mobile, xDSL, cable – and internetworking with legacy IPv4 networks and services, to test the performance of future IPv6 networks, and non-commercial native IPv6 advanced services and applications. The network's Acceptable Use Policy (AUP) excludes the possibility of carrying commercial traffic.

The network has been used and tested by the user groups to validate and assess the feasibility, features and potential of the Next Generation Internet through daily, routine use of the services, internal trials and also in highly visible events and public trials.

The **fourth objective** of the project has been dissemination, liaison and coordination with clusters, fora, standards organizations (e.g. the IETF and RIPE) and third parties, with particular consideration for interworking and coordination with peer projects, such as GÉANT, 6WINIT, LONG, MIND, 6NET and any other projects related to our work, that might be available during the Euro6IX project lifetime.

2.3. Main activities developed

Euro6IX has worked in many scientific aspects related to IPv6, involving a high degree of innovation. We can enumerate some of the key activities:

1. Interoperability and performance testing.
2. Deployment of IPv6 mobility in ISP networks.
3. Address aggregation and delegation in ISP/IX networks.
4. Advancing routing aspects in IXs.
5. Deployment of IPv6 in broadband networks.
6. Deployment of IPv6 multicast.
7. Deployment of QoS in broadband.
8. Evaluation of Authentication, Authorization and Accounting mechanism with IPv6.
9. Deployment of transition mechanisms.
10. Deployment of IPv6 VPNs.
11. Policy Based Management Networks with IPv6.
12. Distributed security with IPv6.

We can conclude indicating that Euro6IX has been key in order to build realistic large-scale IPv6 networks, which provided the necessary expertise in order to allow the next step: The integration of IPv6 in commercial networks in order to provide new business chances for ISPs on the way to a new generation of service and applications which can reestablish the innovation in Internet.

2.4. Partners of the Project

The Euro6IX project has involved the cooperation of the following partners:

- Telefónica I+D
- Consulintel
- Telecom Italia Lab
- Technical University of Madrid
- Telscom
- University of Southampton
- 6WIND
- Vodafone
- T-Systems
- BTexact Technologies
- Ecija & Asociados
- Ericsson Telebit
- Eurocontrol
- France Telecom RD
- novaGnet systems
- PT Inovação
- University of Murcia

More information about the project partners available at
http://www.euro6ix.org/partners/e_partners.php

In addition, two sponsors had also participated in the project:

- Hitachi
- Swisscom Innovations

More information from the sponsors available at
http://www.euro6ix.org/sponsors/e_sponsors.php

3. Security in IPv6 Networks: Introduction, State of the Art and New Challenges

3.1. Introduction

The continuous growth of the Internet requires that its overall architecture evolve to accommodate the new technologies that support the growing number of users, devices, services and applications. IPv6 has been designed as the network protocol to meet with these requirements.

Security has been always mentioned as one of the most interesting added-value services introduced by IPv6, at least in theory. In fact, the deployment of secure communication networks based on IPv6 presents new issues that need to be addressed in labs, but also in real operational IPv6 networks as the one developed as part of the Euro6IX (European IPv6 Internet Exchanges Backbone) EU IST project, where most of the analysis and research work presented here has been carried out.

When speaking about network security in IPv6 communication systems, the main technology that should be mentioned is *IPsec*. In fact, this is the protocol designed and proposed by the IETF and accepted by the international community as de facto standard to provide security at the IP (i.e., both IPv4 and IPv6) layer. The fact of being at the network layer makes it a good solution for several reasons; some of the most relevant are:

- It helps to block many of the low-level traditional attacks as, for example, IP address spoofing or packet sniffing. This represents an important step towards the provision of security in IP networks, as these attacks are usually very easy to implement and at the same time quite effective when performed against unprotected networks.
- It provides a certain set of basic security mechanisms that can be available to all higher-level services and applications. This may help to solve some of the current problems occurring nowadays when different services and applications define and implement their own security solutions that are usually not interoperable and require a certain level of intervention (and training in terms of security) of end users. In this sense, IPsec avoids the duplication of basic security services, such as access control and the provision of confidentiality to a given communication channel. However, it is also important to mention that as IPsec is based on the network layer, it is not a complete solution when the services or applications to be protected are more user-oriented than network-oriented; this can be the case of an e-mail service or an e-/m-commerce application, for example.

In fact, IPsec adds integrity checking, authentication, encryption and replay protection to IP communications. It is used for *end-to-end security* and also for creating *secure tunnels*

between IP gateways. It was also designed for interoperability and it does not affect networks and hosts that do not support it. IPsec is also independent of the current cryptographic algorithms, being able to accommodate new ones as they become available.

Security features in IPsec have been introduced mainly by means of two dedicated components: the *Authentication Header* (AH) and the *Encrypted Security Payload* (ESP). On the one hand, the AH header is used to provide integrity and authentication to IP packets. Reply protection is also possible, although its usage is optional. Its presence protects against two main threads: packet spoofing and the modification of certain fields. On the other hand, the ESP header is used to provide integrity check, authentication, and encryption to IP packets. In this case, optional replay protection is also possible.

The AH and ESP headers can be used in different ways to protect IP communications, as it is the case of *VPNs* (Virtual Private Networks). The main motivation behind them is the fact that the Internet has become a popular, low-cost backbone communications infrastructure, which leads many companies to consider building an extension of their private network through the Internet to communicate different branches or establishing a secure communication channel with their suppliers and clients.

3.2. IPsec and IPv6

As commented before IPsec and its two components (AH and ESP) works with both IPv4 and IPv6. The next question that needs to be clarified is what within IPsec which is directly related with IPv6? Several of the most relevant answers are given here:

- The design of IPsec was part of the deployment of the new IPv6 protocol; in fact, taking a look to IPv4-based communication networks in early 90's they were designed and implemented to work in a friendly environment, which is a hypothesis that is no longer valid as of a few years ago, when these networks started to be used in the commercial domain. As such, IPsec works both with IPv4 and IPv6, but it is defined as a mandatory component to be implemented as part of IPv6 stacks.
- The security features have been defined to be an integrated part of the set of services offered by IPv6 as, for example, QoS or mobility, although this is mostly in theory, as reality shows that integration between these different networking services is still far from being a reality, and much more research work in both the design and implementation parts is required. As an example, the secure management of mobile devices in IPv6 networks is nowadays a very interesting research topic, and still in the phase of identifying scenarios and providing partial solutions to them.

- The flexibility of the IPv6 address schema provides the support for private addresses but will surely reduce the use of NAT (Network Address Translation) boxes because global addresses are widely available. In this sense, IPv6 seems to fully enable *end-to-end security* that is not always available throughout current IPv4 computer networks that use NAT and other techniques for address conversion or temporally allocation. This functionality is considered as very important for emerging services and applications requiring security such as mobile devices, integrated telephony systems, Internet-connected cars, home devices, etc.
- IPv6 security features are implemented using extension headers so they can be easily turned off when security aspects are not relevant or network performance is of a big importance, as it is the case with certain mobile scenarios with a low bandwidth or small devices with certain computing or battery limitations (such as sensor networks).
- IPsec can provide direct protection to other IPv6-related protocols, as ICMPv6 (Internet Control Message Protocol for IPv6).

3.3. Issues to Consider when Enabling Security in IPv6

All these aspects bring several interesting advantages to networking systems. However, there are several issues that should be considered, especially by network designers when enabling security into their IPv6 native or IPv4/IPv6 dual-stack networks. The main reason for this is that the notion of current networks as having a *static* topology, a certain number of *controlled* access points (which are usually implemented with firewalls) and that traffic is mainly in the clear (and just a few packets will be encrypted, but just at the transport and application layers) is no longer a valid assumption.

In fact, enabling IPv6 security means allowing *end-to-end* network authentication and encryption between devices and then limiting very much the capacity of different systems implementing and controlling security policies or doing monitoring functionalities in benefit of the security of the network, such as firewalls or IDS (Intrusion Detection Systems). These tasks can be even more complicated when dealing with secure IPv6 mobility at the same time, as the topology of the network can be changing over time, with mobility requiring host addresses and routing to be (re-)assigned dynamically in time.

This has an important implication over the traditional way of defining security in networks, which is usually based on a first design phase trying to identify the boundaries of the information system (i.e., security domain) and the security policies that should be applied, usually in the security systems placed at the boundary of the network. In this phase, which is very much related with applying network- and transport-level security measures in the

boundary devices, end nodes and users are not usually considered. They are mostly addressed in a later phase with the definition of the application-level measures to take, i.e. the antivirus software to be used or the software updating policy that should be implemented.

However, in IPv6 networks this will most probably change also taking into consideration the enforcement of security measures and policies in the end devices as part of a complete security strategy; this will lead to the distributed management of security inside security domains.

Network security designers will also need to take into account the dynamicity of topology, which is nowadays considered as the basic context to define and evaluate network risks and vulnerabilities, and intrusion detection alarms.

Moreover, the concept of firewalls will need to be updated from their current role of a device implementing filtering, NAT, proxies and port translation for a *static* network topology, to a new device (or a set of them) able to deal with dynamic host addressing and routing, encrypted payloads and not predictable ways to associate a source or destination IP address with a given user. Also IDS systems will need to update the current set of attack signatures to IPv6 and adapt, when possible, to dynamic addressing and limited visibility in the packet data content.

IPv6 and the Right to Privacy

1. Introduction

Dealing with the issue of privacy is fundamental in order to generate consumer confidence and ensure the successful widespread development of IPv6 in Europe. Irrespective of how well IPv6 is designed and how many additional possibilities it provides such as autoconfiguration, more IP addresses, optimized mobility, extensibily, means for better quality of service and security, among others, if people do not have confidence that it will protect their privacy (i.e. think it is unsafe), this will hinder its widespread deployment in Europe. Bad news rather than good news grabs the headlines and therefore if unchallenged stories are published about how IPv6 could allow every aspect of a citizen's life on the Internet to be tracked, it could be easy for this perception to develop in Europe. If this public perception is allowed to take hold, this could cause untold damage to IPv6's deployment.

The bad publicity started in the US during the late 1990's when press reports began to appear about privacy concerns relating to the use of unique serial numbers in IPv6 addresses. The concerns mainly focused on the possibility of monitoring individuals on an unprecedented nature based on tracking their activities through their IPv6 address embedded in every packet of information transmitted.

This debate crossed the Atlantic and both the European Council and the Article 29 Data Protection Working Party of the European Commission have recognized the possibility of similar privacy concerns. This chapter's role is to analyze what the concerns are, how they fit into the current European legal framework, whether these concerns are justified and if so, identify what needs to be done.

2. IPv6 and Privacy

IPv6 has been called the New Internet or the Internet for the New Generation. The problem with the rapid growth in the 'Old' Internet over the last years is that it is running out of addresses. The Internet's basic communications are made possible by a system called IP (which stands for Internet Protocol) which requires every Net connected computer or device to have a digital address called an IP address. The current version of the Internet protocol is called IP version 4 (or IPv4) and this has been used for about 20 years.

Additionally the distribution of the addresses in IPv4 is unbalanced as a third of the world's addresses are reserved for the US where in fact two US universities have more allocated addresses than the whole of China.

The computer scientists who developed the Internet and preside over its basic structure foresaw the address shortage problem and about 10 years ago developed a basic new version of the Internet Protocol called IPv6. This has enough capacity to provide a billion

IPv6 and the Right to Privacy

billion addresses for each square metre of the earth's surface. Mathematically speaking, this has been done by moving from a 32-bit IPv4 address to a 128-bit IPv6 address, which will allow for the predicted future growth of the Internet and Internet related technologies.

A smooth move from IPv4 to IPv6 is a huge task and needs a substantial investment in research and technology so that a large-scale trial for the continuing development and architecture can be conducted on an international level.

Apart from addressing the shortage problem, the development and introduction of IPv6 will allow a general overhaul of the architecture and design of the Internet to create a faster, better quality, more secure service. IPv6 solves the scaling issues of today's Internet and supports new features while enhancing others, including end-to-end connectivity, plug & play autoconfiguration, built-in security, mobility, multicast and support of larger data packets.

Whilst the introduction of the New Internet is both necessary and inevitable, concerns about the design of one type of IPv6 address using unique identifiers may give rise to privacy issues that need to be considered.

2.1. What is Privacy?

Privacy is and has always been one of the most important and comprehensive of all human rights. It is also one of the hardest to protect. Without privacy, other rights like freedom of speech or assembly would be less meaningful.

Privacy has many important aspects. In part, it is what you choose to let other people know about you and in part it is the ability to remain anonymous. Privacy is about who controls the information you choose to share with other people. For example, you might decide to share your address with an on-line bookseller you are buying a book from but you would not want them to publish your address to all visitors to the web page and they would be breaching your privacy if they did so.

In general when we talk about our right to privacy, we mean the right to:

- Keep our personal information to ourselves.
- Have the choice to remain anonymous or unidentified with respect to certain personal and public activities. These activities would include the exercise of public rights like freedom of assembly, or private choices like our spending habits or our manner of worship.
- Live our lives without being under surveillance (or watched) by other people.
- Conduct private communications.
- Have physical privacy and personal space.
- To be left alone, both as consumers and as citizens.

IPv6 and the Right to Privacy

The only way for an individual to guarantee to protect his privacy is to stop interacting with the world. Obviously this is impossible and undesirable for ordinary citizens and therefore general principles needs to be developed to make sure that when interaction took place, some protection was available.

2.2. What is the Foundation for the Right to Privacy?

The modern day basis for European privacy is the European Convention for the Protection of Human Rights and Fundamental Freedoms 1950. The Convention, established by a now defunct body called the Council of Europe and open to any European Country to ratify, was intended to put the protection of human rights and fundamental freedoms on a 'legal' footing following the Second World War. It encompasses a number of fundamental rights such as the right to life, the right to a fair trail, the right against torture and amongst these fundamental rights we also find the right to privacy.

The Convention's definition of the right to privacy (contained in Article 8) extended to four separate areas where an individual has the right to have his privacy respected:

- Private life.
- Family life.
- Home life.
- Correspondence.

This Convention was adopted before the European Community or Union (as we know it today) was formed. However as human rights were one of the founding principles of the EU and an indispensable condition for its legitimacy, the Heads of State or Government decided in a meeting at the Cologne European Council (June 1999) that there was a need to formalize these rights and to ensure that they were more visible within the Union. This led to the proclamation of the EU Charter on Fundamental Rights adopted on 8th December 2000.

The right to privacy as set out in the 1950 Convention was mirrored in Article 7 of the EU Charter that stated:

'Everyone has the right to respect for his or her private and family life, home and communications'.

2.3. What is the Link between Privacy and Data Protection?

Since the 1950 Convention a new facet of privacy had developed, directly linked to technological advances and in particular the increase in the automated processing of information. This new facet of privacy became known as data protection. Data protection is the sword

IPv6 and the Right to Privacy

used to protect privacy in the technological age. Whilst Article 7 of EU Charter 2000 reflected the fundamental right to privacy as enshrined in the 1950 Convention, it also contained a new fundamental right not dealt with in 1950, the right to data protection.

Article 8 of the 2000 EU Charter states that:

1. 'Everyone has the right to the protection of personal data concerning him or her.
2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data, which has been collected concerning him or her, and the right to have it rectified.
3. Compliance with these rules shall be subject to control by an independent authority'.

This chapter does not pretend to include an exhaustive study about data protection, but it is important to bear in mind that the implementation of IPv6 entails implications on data protection. Notwithstanding the foregoing some of these implications will be analyzed briefly in the present chapter. However, the main study on this subject will be treated in the following chapter of this book.

2.4. What Rules Govern Data Protection?

Although this legislation will be analyzed in detail through section 3 of the next Chapter, it could be convenient to state that the genesis of modern data protection legislation can be traced to the first data protection law in the world enacted in the Land of Hesse in Germany in 1970. National laws in Sweden (1973), the United States (1974), Germany (1977), and France (1978) followed.

The first major European legislation was the Council of Europe's 1981 Convention for the Protection of Individuals with regard to the Automatic Processing of Personal Data that set out specific rules covering the handling of electronic data. These rules defined personal data and established the necessary protection at every step from collection to storage and dissemination.

The 1981 Convention effectively forms the basis of modern European thinking on data protection and explicitly created the link between data protection and privacy, basing the protection of personal data on protecting the fundamental human right to privacy (Article 1). The Convention's object was to strengthen data protection, i.e. the legal protection of individuals with regard to automatic processing of personal information relating to them. It aimed to create some rules about how personal information should be treated and how individuals could have control over personal information collected and used by others.

IPv6 and the Right to Privacy

The basic data protection principles established in the 1981 Convention were developed in three subsequent EC Directives.

- Directive 95/46/EC of the European Parliament and the Council of 24th October 1995 on the protection of individuals with regard to the processing of personal data and the free movement of such data.
- Directive 97/66/EC of the European Parliament and the Council of 15th December 1997 concerning the processing of personal data and the protection of privacy in the telecommunications sector.
- Directive 2002/58/EC of the European Parliament and the Council of 12th July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications Sector.

The first Directive established a framework to allow the free movement of data, but at the same time ensure that the fundamental right of privacy was protected. It recognized that continuing advances in technology developed new ways to capture, transmit, manipulate, record and store personal data and therefore was expressly drafted in such a way as to be adaptable and applicable to technological advances.

The legal definition of 'personal data' was expanded from the Convention to encompass '*any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity*.' It is important in this definition to highlight the possibility to consider a number as a mean of identification, under some circumstances.

The Directive established general rules on the lawfulness of the processing of personal data and deals specifically with issues such as the principles relating to data quality, the criteria for making data processing legitimate, special categories of processing, information to be given to the data subject, the data subject's right of access to data, exemptions and restrictions, the data subject's right to object, confidentiality and security of processing, notifications, judicial remedies, liabilities and sanctions, transfers of personal data to third countries, codes of conduct and supervisory authorities.

Article 29 of Directive 95/46/EC also established an independent Working Party whose ambit was inter alia to examine, opine, advise and recommend on how the processing of personal data impacted on the rights and freedoms of natural persons.

Directive 97/66/EC (telecommunications sector) sought to extend the principles of Directive 95/46/EC to the telecommunications networks as the Commission stated that 'new advanced digital technologies are introduced in public telecommunications networks, which give rise

IPv6 and the Right to Privacy

to specific requirements concerning the protection of personal data and privacy of the user and the development of the information society is characterized by the introduction of new telecommunications services'. The use of public telecommunications networks created new 'forms' of data, which did not necessarily fit neatly into the existing data protection definitions and therefore this Directive was a way of ensuring that the legislation dealt adequately with these technological advances.

The Directive above in turn needed to be adapted to take into consideration developments in the Markets and Technologies for Electronic Communications Services in order to provide an equal level of protection of personal data and privacy for users of publicly available electronic communications services, regardless of the technologies used. Therefore Directive 2002/58/EC was adopted as a response to new advanced digital technologies being introduced (e.g., widespread access to digital mobile networks). These advanced digital technologies entailed new possibilities for users but also new risks for their data protection and privacy. The Directive 2002/58/EC sought to provide confidence to users that their privacy will not be at risk with these new developments.

Directive 2002/58/EC did not create major changes to the substance of Directive 97/66/EC. It merely adapted and updated the existing provisions to new developments in electronic communications services and technologies. Therefore, the majority of provisions of the existing Directive were simply carried over in the new proposal. The new regulatory framework was intended to recognize the convergence of telecommunications, media and information technology. It covered all communications infrastructure and associated services and was intended to be technology-neutral. The intention was that the same service is regulated in the same way, regardless of how it is delivered.

Recital 6 of Directive 2002/58/EC states that: *'The Internet is overturning traditional market structures by providing a common global infrastructure for the delivery of a wide range of electronic communications services. Publicly available electronic communications services over the Internet open new possibilities for users but also new risks for their personal data and privacy.'*

The three Directives above taken in conjunction were intended to ensure that there was sufficient protection for any form of automated processing in any technological form. The Internet, and therefore IPv6, will be subject to the Directives and the rules that this imposes(1).

The fundamental principles of data protection extracted all require that personal information must be:

- Obtained fairly and lawfully.
- Used only for the original specified purpose.
- Adequate, relevant and not excessive to purpose.

(1) Article 29 Working Party document on the Processing of Personal Data on the Internet adopted on 23rd February 2003 (WP16).

- Accurate and up to date.
- Accessible to the subject.
- Kept secure.
- Destroyed after its purpose is completed.

As we shall see, those involved in the design and implementation of IPv6 need to bear these principles in mind to ensure that the New Protocol complies with these requirements.

3. What are some of the General Privacy Concerns Regarding the Internet?

3.1. Where are the Inherent Dangers in the Internet Protocol?

To understand the reason for the privacy concerns in the Internet (and IPv6) it is necessary to understand how the Internet works. The Internet is a network of computers communicating with each other on the basis of the Transport Control Protocol/Internet Protocol (TCP/IP). For the Internet Protocol to function and computers to be able to communicate with each other, every computer is identified by a single numerical IP address (in IPv4 this is a 32 bit address and in IPv6 a 128 bit address).

The fact that turns IPv6 into possible problem in terms of privacy and data protection raises from the necessity to know if an IP address could be considered as personal data. This issue will be analyzed in section 2.2. of Chapter III of this book.

In particular, if a direction IP is considered as personal data, then the processing of these personal data will be protected by the norms that regulate the right to privacy and data protection which have been analyzed previously.

3.2. Actors in the Internet

The various participants in the Internet are:

- The software, computer and telecommunications industries that design the network and services available.
- Telecommunications operators who provide the network for data transfer.
- Internet Access provider responsible for the Internet transport system.
- Internet Service Providers, which provide services such as HTTP (often the same as the ISP).
- The user.

Each of these actors has its own data protection and privacy responsibilities and ought to look at their role and the service that they provide to ensure that their actions are privacy and data protection compliant.

A Report and Guidance published by the International Working Group on Data Protection in Telecommunications ('Budapest - Berlin Memorandum on Data Protection and Privacy on the Internet') in 1996 provided a useful overview of Internet privacy concerns for the Internet in general.

The document explained that the vast growth of the Internet had created what can be regarded as the first level of the emerging Global Information Infrastructure (GII) that potentially created numerous problems in relation to privacy. There are various participants in the Internet and each of these has different tasks, interests and opportunities and the principles of privacy and data protection needed to be maintained at all these different stages.

'Given that the Internet does not have one governing body to oversee privacy and data protection issues on a global scale, the 'user is forced to put trust into the security of the entire network, that is every single component of the network, no matter where located or managed by whom'.

The paper stated that there are certain bodies (international, regional or national) that manage various functions on the Net and given the fact that there is no Internet Governing body, the role of these bodies is important, in particular when developing the protocols and standards for the Internet, fixing rules for the identification of servers connected and eventually for the identification of users. This is directly applicable in the context of IPv6.

'A balance has to be struck between a person who does not want to leave his fingerprints on the Net and the fact that providers will want identification and authentication to help with charging and marketing tasks'.

3.3. Privacy Guidelines

The International Working Group on Data Protection in Telecommunications published a 10-point plan as an overview of the principles to be borne in mind regarding this issue.

The 10-point plan stated:

'There can be no doubt that the legal and technical protection of Internet users' privacy is at present insufficient.

On the one hand the right of every individual to use the Information Superhighway without being observed and identified should be guaranteed. On the other hand there have to be limits (crash-barriers) with regard to the use of personal data (e.g. of third persons) on the highway.

IPv6 and the Right to Privacy

A solution to this basic dilemma will have to be found on the following levels:

1. Service providers should inform each potential user of the Net unequivocally about the risks to his privacy. He will then have to balance these risks against the expected benefits.
2. In many instances the decision to enter the Internet and how to use it is subject to legal conditions under national data protection law.
3. Initiatives to arrive at closer international cooperation, even an international convention governing data protection in the context of trans-border networks and services are to be supported.
4. An international oversight mechanism should be established which could build on the existing structures such as the Internet Society and other bodies. Responsibility for privacy protection will have to be institutionalized to a certain extent.
5. National and international law should state unequivocally that the process of communicating (e.g. via electronic mail) is also protected by the secrecy of telecommunications and correspondence.
6. Furthermore it is necessary to develop technical means to improve the user's privacy on the Net. It is mandatory to develop design principles for information and communications technology and multimedia hard and software, which will enable the individual user to control and give him feedback with regard to his personal data. In general users should have the opportunity to access the Internet without having to reveal their identity where personal data are not needed to provide a certain service.
7. Technical means should also be used for the purpose of protecting confidentiality. The use of secure encryption methods must become and remain a legitimate option for any user of the Internet. The Working Group supports new developments of the Internet Protocol (IPv6), which offer means to improve confidentiality by encryption, classification of messages and better authentication procedures. The software manufacturers should implement the new Internet Protocol security standard in their products and providers should support the use of these products as quickly as possible.
8. The Working Group would endorse a study of the feasibility to set up a new procedure of certification issuing 'quality stamps' for providers and products as to their privacy-friendliness. This could lead to an improved transparency for users of the Information Superhighway.
9. Anonymity is an essential additional asset for privacy protection on the Internet. Restrictions on the principle of anonymity should be strictly limited to what is necessary in a democratic society without questioning the principle as such.

IPv6 and the Right to Privacy

10. Finally it will be decisive to find out how self-regulation by way of an expanded 'Netiquette' and privacy-friendly technology might improve the implementation of national and international regulations on privacy protection. It will not suffice to rely on any one of these courses of action: They will have to be combined effectively to arrive at a Global Information Infrastructure that respects the human rights to privacy and to unobserved communications.'

The Article 29 Working Party as well as looking at specific issues regarding the Internet provided some general guidelines. It stated that:

- 'The Internet was conceived as an open network at world level (www) through which information could be shared. It is however necessary to find a balance between the 'open nature' of the Internet and the protection of the personal data of the Internet users (proportionality).
- Enormous amounts of data on Internet users are collected on the Internet while often users are not aware of this fact. This lack of transparency towards the Internet users needs to be addressed in order to achieve a good level of personal data and consumers' protection.
- Protocols are technical means that in fact determine how data are to be collected and processed. Browsers and software applications also play an important role. In some cases they include an identifier that makes it possible to link the Internet user to his/her activities in the Net. It is therefore the responsibility of those involved in the design and development of these products to offer users privacy-compliant products.'

The question of anonymity was specifically dealt with in Recommendation 3/97 Anonymity on Internet dated 3rd December 1997. This stated that:

'Over the past 25 years it has become apparent that one of the greatest threats to this fundamental right to privacy is the ability for organizations to accumulate large amounts of information about individuals, in a digital form which lends itself to high-speed (and now very low-cost) manipulation, alteration and communication to others. Concerns about this development and the potential misuse of such personal data has led all European Member States (and now the Community with Directive 95/46/EC) to adopt specific data protection laws which set down a framework of rules governing the processing of personal information.

A feature of telecommunications networks and of the Internet in particular is their potential to generate a huge quantity of transactional data (the data generated in order to ensure the correct connections). The possibilities for interactive use of the networks (a defining characteristic of many Internet services) increases the amount of transactional data yet further.

IPv6 and the Right to Privacy

As on-line services develop in terms of their sophistication and their popularity, the problem of transactional data will grow. Everywhere we go on the Internet, we leave a digital trace. As more and more aspects of our daily activities are conducted on-line, more and more of what we do, our choices, our preferences, will be recorded.

Transactional data are only a threat to individual privacy if the data relate to an identifiable person. Clearly one way of addressing privacy concerns would therefore be to seek to ensure that wherever feasible the data traces created by using the Internet do not permit the identification of the user. With anonymity guaranteed, individuals would be able to participate in the Internet revolution without fear that their every move was being recorded and information about them accumulated which might be used at a later date for purposes to which they object.'

However the principle of anonymity must be balanced with the 'principle of proportionality'. The Recommendation is that on the key issue of anonymity, the same rules as regard offline behavior should be followed on line.

Finally the Recommendation concludes that:

'The ability to choose to remain anonymous is essential if individuals are to preserve the same protection for their privacy on-line as they currently enjoy off-line.' However this should always be balanced, taking into account other considerations such as prevention of crimes.

More importantly with regard to the Internet Protocols, which has a bearing on IPv6, the Recommendation stated that:

'User access and activity on the Internet is very rarely anonymous..., the technical configuration on Internet protocols does not easily allow true anonymity...'

The Internet posed a problem because 'the use of the infrastructure is often directly based on the processing of personal data, such as certain Internet Protocol addresses'.

4. What are the Specific Privacy Concerns for IPv6?

As mentioned in the introduction, commentators raised concerns about the privacy issues surrounding IPv6 in the United States in the late 90's and these concerns have been officially raised in Europe.

The first official paper was released when the European Commission published COM (2002) 96 dated 21st February 2002. This publication was a communication from the Commission to the Council and the European Parliament entitled 'Next Generation Internet – priorities for action in migrating to the new Internet protocol IPv6'. The aim of this document was to set

IPv6 and the Right to Privacy

out the European Commission's views on issues concerning the deployment of IPv6 in Europe and one of the issues specifically dealt with was privacy.

The European Commission's thinking is highlighted in the following paragraph:

'However for new Internet enabled services to be deployed in a timely manner, it is of key importance to structure, consolidate and integrate European efforts on IPv6, and notably to develop the necessary base of skilled human resources, to fully harmonize, where needed, the policy approaches, to sustain the research effort, to promote the standards and specifications work and to ensure that all sectors of the new economy likely to be impacted by IPv6 are fully aware of potential benefits accruing from its adoption.

Also, the Commission proposes a set of actions to ensure that the European Union maintains the initiative and leadership in these global developments. These actions require a concerted action aiming at the structuring, consolidation and integration of European efforts on IPv6, notably through:

1. An increased support towards IPv6 in public networks and services.
2. The establishment and launch of educational programmes on IPv6.
3. The adoption of IPv6 through awareness raising campaigns.
4. The continued stimulation of the Internet take-up across the European Union.
5. An increased support to IPv6 activities in the 6th Framework Programme.
6. The strengthening of the support towards the IPv6 enabling of national and European Research Networks.
7. An active contribution towards the promotion of IPv6 standards work.
8. The integration of IPv6 in all strategic plans concerning the use of new Internet Services.'

Having set out the background, the Communication specifically deals with the potential privacy issues for IPv6.

'Due to the fact that the Internet has, from the very beginning, been considered as an open network, there are many characteristics of its communication protocols, which, more by accident than design can lead to an invasion of the privacy of Internet users. Concerns are expressed on a regular basis regarding the need to find a balance between the 'open nature' of the Internet and the conflicting needs to effectively maintaining and debugging a network and the protection of the personal data of the Internet users. The fundamental right to privacy and data protection is enshrined in the EU Charter on fundamental rights and developed in detail in the EU data protection directives 95/46/EC and 97/66/EC which both apply to processing of personal data on the Internet. In its Communication on the Organization and

Management of the Internet Domain Name System of April 2000, the Commission stated already that an IP address can be personal data in the sense of the legal framework (for example dynamic IP addresses). Also the Article 29 Data Protection Working Party, the independent EU advisory body on data protection and privacy established by Directive 95/46/EC, draws the attention at several occasions to privacy issues raised by the use of the Internet. The Article 29 Data Protection Working Party as well as the International Working Group on Data Protection in Telecommunications (the 'Berlin Group') work specifically on IPv6.

It is therefore of indispensable that the European Commission and the European Union as a whole consider privacy issues in the further development of Internet. While privacy issues are currently being taken into account in the development of IPv6, it is essential that the trust and confidence of Internet users in the whole system, including in the respect of their fundamental rights, is ensured'.

In its conclusions the European Commission asked for the parties to:

'Study the impact of the further evolution of the Internet including the new generation IPv6 protocol, on the fundamental right to privacy and data protection, so as to ensure that the required standards and specifications take these aspects into full consideration'.

Having called for a general study into the privacy issues, a few months later in May 2002, the Article 29 Working Party published a document entitled 'Opinion 2/2002 on the use of unique identifiers in telecommunications terminal equipment: The example of IPv6'.

This paper highlights the danger to privacy in respect of 'the possibility of the integration of an unique identifier number in the IP address as designed according to the new protocol'.

The thrust of this paper is that IP addresses attributed to Internet Users are personal data and therefore they are subject to the guidelines provided in the EU Directives.

5. What is the Basis for these Privacy Concerns?

The privacy concerns highlighted in section 4 above are based on one design of the addressing format in IPv6 as approved by the Internet Engineering Task Force. This is the technical body advising on how the Internet should be developed and it provides standards for the Internet through the publication of various technical standards known as RFCs.

5.1. Request for Comments (RFC)

The Requests for Comments (RFC) document series originated as a set of technical and organizational notes about the Internet. Memos in the RFC series discussed many aspects of computer networking, including protocols, procedures, programs and concepts. These official

IPv6 and the Right to Privacy

specification documents of the Internet Protocol defined by the Internet Engineering Task Force (IETF) and the Internet Engineering Steering Group (IESG) gained increasing importance and were recorded and published as standards track RFCs. This meant that RFCs became unofficial standards about how the Internet should be developed. As a result, the RFC publication process plays an important role in the Internet standards process. RFCs must first be published as Internet Drafts so that experts in the relevant areas have an opportunity to comment on the issue at hand before a consensus on the way forward is reached and the RFC becomes a standard.

The simple procedure is that in practice the specification undergoes a period of development and several iterations of a review by the Internet community and eventually is adopted as a standard by the appropriate body.

There are three maturity levels for RFC:

- Proposed Standard.
- Draft Standard.
- Standard.

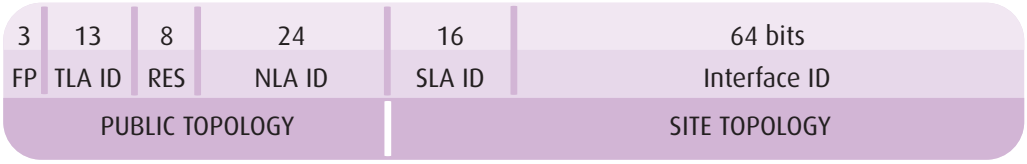
5.2. Does an IPv6 Address have a Unique Identifier?

There are various different types of addresses in IPv6 but the privacy issue relates to the address generated by stateless address autoconfiguration. The technical detail, which explains how this works, can be found in the following documents - RFC2373 relating to the IPv6 addressing architecture, RFC2642 entitled 'IPv6 Stateless Address Autoconfiguration' and RFC2374 titled 'IPv6 Aggregatable Global Unicast Address Format' and subsequent documents (draft-ietf-ipv6-unicast-aggr-v2-02.txt). We do not propose dealing with the technical intricacies of addressing but explain in simplistic terms how this type of address is created and whether the privacy concerns about unique identifiers are justified.

The rationale behind stateless address autoconfiguration is to generate a global unique address without the need for a DHCP (Dynamic Host Configuration Protocol) server. DHCP is the protocol, which allows a network administrator to supervise, manage centrally and automate the assignment of IP addresses. Using the analogy of postal address, the common standard is to put the name of the recipient, followed by the street (including number), city, state, post or zip code and country.

This standard is now globally accepted and used in traditional postal correspondence. There is a similar standard or formula for the new IPv6 addresses in order to allocate the 128-bit address.

IPv6 and the Right to Privacy



IPv6 Aggregatable Global Unicast Address Format

The numbers in the first line of the table refer to the 'bits'. Each of the bits relates to a different layer to enable communication on the network. The address is split into two parts the public topology and the site topology. Therefore the site would be 'private' depending on each individual network and the public topology relates to the 'public' network to allow Internet communication.

Each of the relevant parts are explained below

FP	Format Prefix (001)
TLA ID	Top-Level Aggregation Identifiers (TLA ID) are the top level in the routing hierarchy. The routing topology at all levels must be designed to minimize the number of routes into the routing tables. Each organization assigned a TLA ID receives 24 bits of NLA ID space. This space can be delegated to approximately as many organizations as the current IPv4 Internet. Organizations assigned a TLA ID can provide service to organizations providing public transit service and to organizations, which do not provide public transit service. The organizations receiving an NLA ID may also choose to delegate their space to another NLA ID's.
Res	The Reserved field is reserved for future use and must be set to zero.
NLA ID	Next Level Aggregation Identifier is used by organizations assigned a TLA ID to create an addressing hierarchy and to identify sites. The organization can assign the top part of the NLA ID in a manner to create an addressing hierarchy appropriate to its network.
SLA ID	Site-Level Aggregation Identifier The SLA ID field is used by an individual organization to create its own local addressing hierarchy and to identify subnets. It is a 16-bit field, so it supports 65,535 subnets. The approach chosen for structuring an SLA ID field is the responsibility of the individual organization.
Interface ID	Interface identifiers are unique serial numbers or addresses that are link dependent and therefore used to identify interfaces on a link. They are required to be unique on that link. It is this part of the address which caused the privacy

IPv6 and the Right to Privacy

Interface ID concerns as we shall see below. An interface is defined as a node's attachment to a link. Interface Identifiers are unique serial numbers or addresses, which are link dependent. An identifier for an interface is (at least) unique per link.

In the last IETF documents, this has been simplified as:

Updated IPv6 Aggregatable Global Unicast Address Format

IPv6 uses the 128 bits to provide addressing, routing, and identification information on a computer interface or network card. Some IPv6 systems use the right 64 bits to store an IEEE defined global identifier (EUI64). This identifier is composed of company id value assigned to a manufacturer by the IEEE Registration Authority. The 64-bit identifier is a concatenation of the 24-bit company identification value and a 40-bit extension identifier assigned by the organization with that company identification assignment. The 48-bit MAC address of a network interface card may also be used to make up the EUI64.

The problems relating to privacy were grounded on the basis that the Interface ID, which would be based on the ID of the hardware interface as described above, would identify each machine individually. Therefore every time one went on the Internet to send and receive packets of information, this would effectively leave a fingerprint which can be traced back to the individual.

5.3. How is an IPv6 Address Configured?

RFC2642 explains how stateless address autoconfiguration combines an interface identifier with a prefix to form an address.

The RFC states:

'This document specifies the steps a host takes in deciding how to autoconfigure its interfaces in IP version 6. The autoconfiguration process includes creating a link-local address and verifying its uniqueness on a link, determining what information should be autoconfigured (addresses, other information, or both), and in the case of addresses, whether they should be obtained through the stateless mechanism, the stateful mechanism, or both. This document defines the process for generating a link-local address, the process for generating site-local and global addresses via stateless address autoconfiguration, and the Duplicate Address Detection (DAD) procedure'.

IPv6 and the Right to Privacy

'One of the design goals for stateless autoconfiguration is that:

- Manual configuration of individual machines before connecting them to the network should not be required. Consequently, a mechanism is needed that allows a host to obtain or create unique addresses for each of its interfaces. Address autoconfiguration assumes that each interface can provide a unique identifier for that interface (i.e., an 'interface identifier'). In the simplest case, an interface identifier consists of the interface's link-layer address. An interface identifier can be combined with a prefix to form an address.'

In layman's terms this RFC outlines further how this type of addresses under IPv6 is self-generating rather than allocated and based on the unique identifiers in the hardware.

5.4. What is the Problem with Stateless Address Autoconfiguration?

The potential privacy problem with this type of IPv6 addresses is described in detail in RFC3041. The document highlights the fact that any communication system which has a constant address or identifier for incoming and outgoing communication has potential privacy concerns (this is the same for IPv4 or IPv6).

'Stateless address autoconfiguration defines how an IPv6 node generates addresses without the need for a DHCP server. Some types of network interfaces come with an embedded IEEE Identifier (i.e., a link-layer MAC address), and in those cases stateless address autoconfiguration uses the IEEE identifier to generate a 64-bit interface identifier. By design, the interface identifier is likely to be globally unique when generated in this fashion. The interface identifier is in turn appended to a prefix to form a 128-bit IPv6 address.

All nodes combine interface identifiers (whether derived from an IEEE identifier or generated through some other technique) with the reserved link-local prefix to generate link-local addresses for their attached interfaces. Additional addresses, including site-local and global-scope addresses, are then created by combining prefixes advertised in Router Advertisements via Neighbour Discovery with the interface identifier.

Not all nodes and interfaces contain IEEE identifiers. In such cases, an interface identifier is generated through some other means (e.g., at random), and the resultant interface identifier is not globally unique and may also change over time. The focus of this document (RFC3041) is on addresses derived from IEEE identifiers, as the concern being addressed exists only in those cases where the interface identifier is globally unique and non-changing'.

RFC3041 spells out the potential privacy problem with the use of the unique identifier as a constant part of the address in the following manner.

IPv6 and the Right to Privacy

The use of a non-changing interface identifier to form addresses is a specific instance of the more general case where a constant identifier is reused over an extended period of time and in multiple independent activities. Anytime the same identifier is used in multiple contexts, it becomes possible for that identifier to be used to correlate seemingly unrelated activity. For example, a network sniffer placed strategically on a link across which all traffic to/from a particular host crosses could keep track of which destinations a node communicated with and at what times. Such information can in some cases be used to infer things, such as what hours an employee was active, when someone is at home, etc.

Web browsers and servers typically exchange 'cookies' with each other. Cookies allow web servers to correlate a current activity with a previous activity. One common usage is to send back targeted advertising to a user by using the cookie supplied by the browser to identify what earlier queries had been made (e.g., for what type of information). Based on the earlier queries, advertisements can be targeted to match the (assumed) interests of the end-user.

The use of a constant identifier within an address is of special concern because addresses are a fundamental requirement of communication and cannot easily be hidden from eavesdroppers and other parties. Even when higher layers encrypt their payloads, addresses in packet headers appear in the clear. Consequently, if a mobile host (e.g., laptop) accessed the network from several different locations, an eavesdropper might be able to track the movement of that mobile host from place to place, even if the upper layer payloads were encrypted.

5.4.1. The Concern With IPv6 Addresses

The division of IPv6 addresses into distinct topology and interface identifier portions raises an issue new to IPv6, which is that a fixed portion of an IPv6 address (i.e., the interface identifier) can contain an identifier that remains constant even when the topology portion of an address changes (e.g., as the result of connecting to a different part of the Internet). In IPv4, when an address changes, the entire address (including the local part of the address) usually changes.

If addresses are generated from an interface identifier, a home user's address could contain an interface identifier that remains the same from one dialup session to the next, even if the rest of the address changes.

A more troubling case concerns mobile devices (e.g., laptops, PDAs, etc.) that move topologically within the Internet. Whenever they move (in the absence of technology such as mobile IP), they form new addresses for their current topological point of attachment. The 'road warrior' who has Internet connectivity both at home and at the office typifies this today. While the node's address changes as it moves, however, the interface identifier contained within the address remains the same (when derived from an IEEE Identifier). In such cases, the interface identifier can be used to track the movement and usage of

a particular machine. For example, a server that logs usage information together with a source address is also recording the interface identifier since it is embedded within an address. Consequently, any data-mining technique that correlates activity based on addresses could easily be extended to do the same using the interface identifier.

6. Do these Privacy Concerns have a Solution?

6.1. RFC3041– Privacy Extensions for Stateless Address Autoconfiguration

RFC3041 'Privacy Extensions for Stateless Address Autoconfiguration in IPv6' is a technical proposed standard that is considered to be, at present, a technical solution to the possible risks that, with regard to the privacy and data protection, might exist as consequence of the use of the new Protocol IPv6.

This RFC establishes a system of two addresses used by the terminal equipment: An address which is used for entering communications, so the terminal interface is always reachable using its permanent address; and another one, generated on a pseudo random basis, used by the terminal for outgoing communications. Hereby, through RFC3041, in general terms, when the communications are generated by the user who is responsible for the connection, his IP address would not be traceable by a non authorized third party (eavesdropper).

In this sense, RFC3041, its operation and utilities will be analyzed in Chapter III of this book.

7. Conclusions

This section sets out the principal conclusions of this study regarding the implications on privacy of the implementation and use of the new Protocol IPv6:

1. The implementation of IPv6 is important to the technological competitiveness of Europe. However whilst the rapid deployment of IPv6 should be encouraged, this should not be at the expense of safeguarding certain important principles.
2. The right to privacy and the right to data protection are two fundamental rights enshrined in the EU Charter and legislation. The protection of these rights is of paramount importance. Technology moves at a fast rate but the European data protection legislation in place is intended to provide checks and balances to protect privacy whilst allowing the development and deployment of new technology.
3. On a general level, designers of new protocols are under a duty to bear the privacy and data protection principles in mind and to ensure that new protocols are privacy compliant. One aspect of privacy and data protection is to allow anonymity for citizens, although this principle of anonymity is balanced with the ability to identify people in order to prevent illegal activity.

Personal Data Protection

1. Introduction

The main reason for the study on data protection contained in this Chapter, is the fact that the current data protection legislation is being consolidated and it is becoming known by companies, organizations and citizens who are acquiring a wide knowledge about their rights and obligations according to this data protection legal framework.

This fact, undoubtedly, is one of the principal reasons to closely study any aspect concerning the implementation and use of IPv6 so that this Protocol can be promoted as a safe option which guarantees the confidentiality of its potential user's personal information, the only way for its implementation to be deemed successful.

The purpose of this Chapter, though it is closely linked to right to privacy, is to analyze the possible implications that IPv6 might have on data protection, as consequence of the possible consideration of IP addresses as personal data on certain occasions, as it has been stated in previous Chapters.

In this respect, it is necessary to explain that although data protection is normally included inside the wider sphere that constitutes the right to privacy, it is a specific legal branch of this area that focuses on ensuring that the processing or use of personal data in respect of a natural person (called data subject) should be carried out in conformity with the existing laws.

Therefore, this Chapter centres, first of all, on analyzing the current European legislation on data protection with the purpose of deciding if it contemplates and regulates the possible problems from the implementation of IPv6 or if, on the contrary, some modification or adjustment to the data protection legislation is necessary.

Secondly, another purpose of this Chapter is to identify some possible problems caused by the introduction of IPv6 in relation to data protection legislation, as well as the adoption of certain technical solutions that have been developed in order to preserve the privacy of the users of this Protocol, specially, based on the RFC3041.

Finally, a brief reference will be presented concerning the problem of the extraterritoriality and the difficulty of adopting a unique legislation that solves the problems that arise in the Internet, regulates certain 'offences' and unifies useful criteria on data protection legislation.

2. What is a Data Protection?

2.1. Definition of Data Protection

Nowadays, the concept 'Data Protection' is a fundamental right of every natural person, also known as the 'right to self-determination of information'.

Personal Data Protection

This right refers to the protection that must be offered and guaranteed to the citizens (natural persons) as consequence of the processing of their personal information (personal data) carried out by a third party in an unauthorized way. This concept is also defined as *'the legal protection offered to a natural person regarding the automatic processing of his personal information'*.

The need for the adoption of some measures to guarantee this protection has been promoted as a consequence of the advance of new technologies that allow the processing of any kind of personal data, by different agents and in a multitude of different situations, thus creating certain insecurity for the data subjects.

The right to data protection allows data subjects to decide what can be done with their personal information and to obtain the sufficient guarantees that the processing of their personal data will be carried out under the data protection legal framework.

In this respect, article 8 of the EU Charter on Fundamental Rights, adopted on December 8th, 2000, recognizes the right of all citizens to the protection of their personal information so that processing this information must be done stating specified motives and always based on the previous consent of the data subject or in compliance with data protection legality.

2.2. Consideration of the IP Address as Personal Data

The purpose of this section, as it has been determined through other Chapters of this publication, is to determine if an IP address can be considered as personal data. In order to do this, various basic concepts need to be observed.

The Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, adopted on 28th January, 1981 of the Council of Europe (known as the Convention 108) defines 'personal data' as follows: *'any information relating to an identified or identifiable individual (data subject)'.*

In the same way, article 2 (a) of the Directive 95/46/EC of the European Parliament and of the Council adopted October 24th, 1995, on the protection of individuals with regard to the processing of personal data and on the free movement of such data, considers 'personal data' as *'any information relating to an identified or identifiable natural person (data subject); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity'.*

Therefore, there are two essential elements that must exist in order to consider certain information as personal data:

- The data subject must be a natural person, not a legal person.
- The possibility of associating the information with the natural person who is the owner of that information, directly or indirectly.

Next, it is necessary to deduce if it is possible to link this provided information with a natural person who is already identified or who could be identified in the future (by reasonable means). Then, it could be understood that the above mentioned information is personal data and, therefore, its processing has to be carried out in conformity with the requirements determined by the current legislation on data protection.

Recital 26 of Directive 95/46/EC states that to determine whether a person is identifiable, account should be taken of all means likely reasonably to be used either by the controller or by any other person to identify the said person.

Likewise, another essential concept which helps to understand this regulation is the concept of 'processing of personal data'. It is important to highlight that what is being regulated by this legislation is the processing of personal information. The mere fact of being a data subject, in principle, does not oblige the subject in any way but rather grants a series of rights relating to his personal data. Nevertheless, when a third party processes this kind of information belonging to a data subject, it becomes a situation relevant for regulation by the previously mentioned legislation.

In that case, Directive 95/46/EC explains in article 2 b), the meaning of the concept 'processing of personal data' as *'any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction.'*

Bearing these considerations in mind, an IP address might be considered personal data because of its numerical nature, which the entity or person who is processing might potentially relate it to a certain user who might be a natural person. For example, an Internet access provider might relate an IP address to one of its users receiving one of its services.

Article 29 Working Party's has stated that as 'recital 26 of Directive 95/46 specifies, data is qualified as personal data as soon as a link can be established with the identity of the data subject (in this case, the user of the IP address) by the controller or any person using reasonable means. In the case of IP addresses the ISP is always able to make a link between the user identity and the IP addresses and so may other parties, for instance by making use of available registers of allocated IP addresses or by using other existing technical means.'

The possibility of associating personal data and a concrete person is increased, in principle, with the use of IPv6 due to the following situation. Some IP addresses created on the basis of this version 6 of the Protocol possibly including an identifying part (Interface ID or Unique Identifier: 64 bits) would identify unequivocally an interface on its terminal (PC, portable computer, PDA's, etc) which, at the same time, might end up being associated with a certain user using different mechanisms (i.e. public guides, public databases like the Whois Database).

Personal Data Protection

It is important to highlight that the implications on data protection that might exist from using IPv6 do not arise exclusively because of the fact that the IP address could be associated with an individual but because it can also be considered as a 'record of personal identification' of the individual and the work or activities that he carries out. In this respect, there might exist a large quantity of information that could be associated to an IP address, for example, information about: A user's purchases, conduct, personal information, etc.

2.2.1. In all cases, could an IP address based on a Unique Identifier be considered personal data?

In general terms, if IP addresses are based on the new version 6 of the Protocol and contain in their configuration a Unique Identifier, it is important to highlight that not in all cases do they have to be considered as personal data. In order to verify this possibility, it is necessary to associate the IP address with a certain natural person. This option will be explained later in this publication.

The following situation is an example of a likely connection between IP address and user. A personal computer is connected to the Internet using the Protocol IPv6. In this respect, the user, using his terminal, would access the Net only with his IP address and its Unique Identifier, which forms part of that address. In this case, the IP address would be directly linked to his terminal and could possibly be linked, indirectly, to the user.

Given that the Internet Service Provider has the possibility of associating the IP address with the holder of this address due to his contract with this services provider, there exists the probable connection of service to user, by fault of the provider, and thus the IP address of the user would be clearly considered as personal data.

On the contrary, the same example shows a situation where the computer used to access to the Net belongs to a Cybercafe, thus the user, who accesses using the above mentioned IP address, changes frequently. In this second situation, the Internet Service Provider might not be able to associate the IP address with the concrete user who is surfing the Net. Therefore, the IP address would not be regarded as personal data.

2.2.2. Could the IP addresses based on a Unique Identifier corresponding to the workplace be considered personal data?

There exists the doubt to whether an IP address that identifies a certain working device or computer in a company might be categorized as personal data or not. This doubt is based on the supposition that the activities undertaken whilst using this IP address will not be included in the private sphere of it's user. In other words, it is assumed that an IP address which belongs to a person and is used for private purposes *must* be considered as personal data. On the other hand, the IP of a workplace is not included in this category of data because it does not belong to the private sphere of the user.

This assessment is not adequate from the point of view of the data protection legislation since the only valid criteria to determine if an IP address is personal data or not is its connection with the natural person who directs the node or the terminal that is accessing the Net.

With regard to the likelihood of relating an IP address to a concrete natural person, it is necessary to examine the further limitations to this aspect of IP addresses, presented in later sections of this publication. This is because certain providers (in forward, agents, providers or actors) could be making this relation of IP address and user directly, whereas other providers would not have this option or would have to come to alternative means of achieving this association.

3. Data Protection Legislation

The aim of this section is to give a brief analysis of the Directives and more important European agreements and conventions on data protection which might be applied initially to IPv6.

However, it appears repetitive to address this analysis and others regarding the progression of the different existing legal frameworks on this matter and previous studies on data protection conducted in different States, since this information was already provided in Chapter II of this publication.

That being said, the principal purpose put forth in the following sections, is to analyze the current legislation on data protection, examining the three following elements:

- To study the current processing and regulation of personal data in Europe by the analysis of the most important legislation on this matter.
- To observe how the Member States have included this framework in their legal systems, highlighting those which should be considered most important.
- To conclude if IPv6 is perfectly regularized by the current legislation or if there are some specifics that would have to be considered by this legislation.

3.1. Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, of the European Council, adopted the 28th January, 1981

This Convention, also known as Convention 108, is a representation of one of the first efforts carried out for the creation and expansion of the legislations on data protection, inclined to regularize the processing of personal information. According to this Convention, the signatory States were required to include in their legal systems the necessary measures and guarantees to concrete the basic principles on data protection.

Personal Data Protection

In few words, the purpose of this Convention is *'to secure in the territory of each Party for every individual, whatever his nationality or residence, respect for his rights and fundamental freedoms, and in particular his right to privacy with regard to automatic processing of personal data relating to him'.*

3.2. Directive 95/46/EC of the European Parliament and of the Council of 24th October 1995, on the protection of individuals with regard to the processing of personal data and on the free movement of such data

Directive 95/46/EC was enforced in 1995, some years after the signature of Convention 108, with the aim to establish the basic principles on data protection which each Member State must incorporate into their domestic legal system. Thereby, it was created as a common and homogeneous legal framework for the European Union relating to this matter. As it states in the Preliminary Consideration Number 25, its purpose is to guarantee the protection of all the personal data, automatic processed by public or private entities and organizations.

As its principle goal, it establishes the following: *'the principles of protection must be reflected, on the one hand, in the obligations imposed on persons, public authorities, enterprises, agencies or other bodies responsible for processing, in particular regarding data quality, technical security, notification to the supervisory authority, and the circumstances under which processing can be carried out, and, on the other hand, in the right conferred on individuals, the data on whom the subject of processing are, to be informed that processing in taking place, to consult the data, to request corrections and even to object to processing, in certain circumstances'.*

3.3. Directive 97/66/EC of the European Parliament and of the Council of 15th December 1997 concerning the processing of personal data data and the protection of privacy in the telecommunications sector

Keeping in mind the multitude of new digital public telecommunications networks and the important processing of personal data carried out by these telecommunications companies, this Directive was published in order to define the basic principles that should govern the specific data processing taking place in this sector.

In effect, some of these aspects include the following:

- The processing of traffic and billing data.
- Itemized billing.
- Presentation and limitation of the identification of the calling and connected line.
- Public directories.

As can be seen, Directive 97/66´s main objective is detailed more specific in comparison to that of Directive 95/46/EC, which puts forth a more general legal framework. Directive 97/66 aims to solve *concrete* problems of this sector which, in numerous occasions, might serve as criteria to resolve possible problems detected in relation to IPv6. An example may be regulating the limitation of the identification of the calling line or the regulation of public directories in general.

Nevertheless, this Directive has been repealed by the recent Directive 2002/58/EC. In spite of this latter Directive extending its legislation to the whole frame of data protection in relation with new technologies (telecommunications and electronic communications, in general), it supports part of the legislation already established in the Directive 97/66/EC.

3.4. Directive 2002/58/EC of the European Parliament and of the Council of 12th July 2002, concerning the processing of personal data and the protection of privacy in the electronic communications sector

As previously mentioned, Directive 2002/58/EC repealed Directive 97/66, further intending to specify the legislation given by the Directive 95/46/EC for the particular sector of the electronic communications according to its articles.

This legal framework aims to protect and safeguard the privacy of the subscribers and users of services of electronic communications. Principally, this Directive regulates the following aspects:

- Technical and organizational safety measures that must be adopted by the providers of electronic communications services.
- Confidentiality of the communications.
- Processing of traffic data.
- Itemized billing.
- Presentation and restriction of calling and connected line identification.
- Processing of location data.
- Directories of subscribers, etc.

3.5. Domestic Legal Systems on Data Protection Adopted by the Member States

As a result of the Preliminary Consideration Number 22 and article 32 of the Directive 95/46/EC, the Member States were bound to adapt their domestic legislations to the principles and obligations regarding the processing of personal data, taken under this Directive. In compliance of this duty, the different Member States have been adopting their own domestic regulations tending to regulate these aspects. Some of these domestic legislations will be analyzed in Section 4.3 of this publication.

Personal Data Protection

4. Data Protection Legislation with Regard to the Use of IPv6

This section focuses on analyzing the adequacy of the previously mentioned Directives (which already have been analyzed in Chapter II) at the moment of using IPv6 to determine the effectiveness of these Directives in terms of detecting new aspects that may develop as a consequence of implementing IPv6 or, if lacking effectiveness, there should be modifications to the Directives.

In particular, this analysis will focus on two specific Directives: 1) Directive 95/46/EC as it is considered the principal legislation on data protection and 2) Directive 2002/58/EC because of its significant contribution to the electronic communications sector, precisely where the new Internet Protocol, version 6, can be categorized. Finally, some brief considerations will be gathered about the adequacy of the domestic regulations on data protection adopted by the different Member States.

4.1. Directive 95/46/EC

The analysis of this Directive will centre on three fundamental existing aspects on the processing of personal data and, thus, on the processing of IP addresses data:

- Obtaining the IP address data.
- Processing of this data by the agents being capable of associating IP address data with a machine and even a user.
- Cancellation and suppression of the IP address information.

Regarding each of these steps for the general act of processing personal information, the legislation for such an act requires certain principles and obligations that any processing agent would have to fulfill.

That being said, this section examines whether the processing of the information of IP addresses could be done in conformity with the legislation provided by the Directive, keeping in mind the above three aspects, and if so, whether it is possible to achieve such an aim under the existing IPv6.

4.1.1. Collection of IP addresses data

The following are the three main principles stated in the legislation which have to be considered when someone (the agent or the collector) proceeds to obtain personal information from any other person: Quality of the information; duty of information and obtaining the appropriate data subject's consent.

Personal Data Protection

Regarding the **principle of data quality**, article 6 establishes the obligation that personal data must be collected and processed as follows:

- Processed fairly and lawfully
- Collected for specified, explicit and legitimate purposes
- Not to be further processed in an incompatible way with those purposes
- Data must be adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed
- Data must be accurate and kept current
- Data must be kept in a form which permits the identification of data subjects for no longer than is needed for which the data were collected or for which they are further processed

This article obligates that all processing of the IP data itself (when it is considered as personal data) and of other personal data which could be related to an IP address, have to be activities that must conform to these basic principles.

Regarding the **information to be given to the data subject**, article 10 enumerates different aspects which the data subject must be informed about, by way of the data collector:

- The identity of the controller and of his representative, if any
- The purposes of the processing of the personal data
- Recipients or categories of recipients of the data
- If the reply to the questions is obligatory or voluntary, as well as the possible consequences of failure to reply
- The existence of the right of access to the data and the right to rectify

The moment when the collector obtains the information of the IP address itself and the information that potentially could be associated with this IP address, the collector will have to inform the data subject about these aspects.

The main problem is that this article is applied when the data subject gives his personal information to the collector personally, but there also exists the possibility, in certain cases, that the data subject gives his IP address while surfing the Net and, therefore, without being fully conscious of sharing this information. In this case, it is questioned who is obliged to inform the parties about the situation and in which appropriate way.

Though the answer to this problem should be analyzed case by case, a general answer would suppose that every natural or legal person while surfing the Net, sending emails or receiving communications, for example, becomes familiar with his IP address, processes it,

stores it and is able to associate this IP to its owner, thus being held to the legislation as well as by the rest of the requirements of the Directive.

On the other hand, article 11 refers to the suppositions in which it is necessary to observe this legislation though the personal data is not obtained directly from the user. A case in point example is one in which the collection of the IP address, as well as the information associated with it, is given by an Internet Access Provider to a company dedicated to the elaboration of consumers profiles.

As can be seen, these articles establish obligations that could be difficult to observe according to the different agents that process personal data. In this respect, section 5 examines how an IP address may, at first, be associated with its holder by an Internet Access Provider. Nevertheless, there might exist other series of agents (i.e. a provider of services of virtual shop) that by reasonable means (public guides, databases, etc) have the possibility of associating the IP with its holder. In these cases, the problem is deciding who will have to comply with this duty of information: the access provider; the provider of the services of virtual shop or both of them.

Finally, regarding the **necessity of obtaining the consent** of the data subject to process his personal data (in this case, his IP address and the data related to that IP address), article 7 of the Directive states that personal data only could be processed when:

- The data subject has unambiguously given his consent (explicit consent, in a few cases and tacit, in others)
- Processing is necessary for the performance of a contract to which the data subject is considered as a party
- Processing is necessary for compliance with a legal obligation
- Processing is necessary in order to protect the vital interest of the data subject
- Processing is necessary for the purposes of the legitimate interests pursued by the controller or by the third party to whom the data are disclosed

In short, the processing of this kind of information will have to be carried out with the data subject's consent or when at least one of the pointed circumstances takes place. In any case, these circumstances could be increased by the different national regulations adopted by the Member States.

Also, article 8 of this Directive determines special requirements for the processing of some categories of data. These categories are racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, health or sexual orientation. For example, these types of special data could be contained in the information that could potentially be related to a concrete IP address.

In that sense, this Directive bans the processing of these categories of data unless it is based on one of the exceptions described in this article. Some of these exceptions are: Obtaining the explicit consent of the data subject, the processing being necessary for the purposes of carrying out the obligations and specific rights of the controller in the field of employment law, the processing being necessary to protect vital interests of the data subject or another person, etc.

These considerations are relevant from the point of view of certain suppositions in which, for example, a service provider could have access to this type of information. An example could be a provider of erotic contents who has a web page which the users can access. If a user is accessing with an IP based on a Unique Identifier, this provider could have information about the sexual contents that this user is accessing and, moreover, he could have the possibility of associating this IP with the machine and, potentially, with the user. In this case, the processing of sexual orientation information associated with an IP and with a user would take place and, therefore, would be bound to the obligations within this article.

4.1.2. IP data processing

Once the personal data are obtained (the IP address itself and, in some cases, another personal information that could be associated with this IP address), the Directive foresees another series of articles intending to regularize these same situations of data processing.

These articles establish the obligation for the agents to adopt some legal, technical and organizational measures to assure the confidentiality, integrity and safety of the personal information. However, the Directive does not establish the type of technical measures to implement, so the domestic legislation of the Member States should determine them. Furthermore, this Directive establishes how the processing of personal data should be executed by third parties.

4.1.3. Cancellation or conservation of the information of IP address

The Directive does not clearly declare which are the requirements that must be highlighted to proceed to the cancellation or to the conservation of personal data. Therefore, it is not possible to know how much time the information regarding IP addresses must remain in the different agents' files and systems or in what cases they would have to be cancelled.

Therefore, it would be necessary to analyze the considerations made by each of the different domestic legislations in order to be able to determine, with certain accuracy, the mentioned time period of conservation of data in light of the remaining parts to the legislation that will be applicable to every supposition of conservation of information.

Personal Data Protection

4.1.4. Must Directive 95/46/EC be modified because of the implementation of IPv6?

It is indisputable that one of the principal debates generated as a consequence of the future utilization of IPv6 remains the probable necessity of modifying this Directive to adapt it to new problems that could be caused by implementing this Protocol or, on the contrary, the probability that this regulation is suitable for IPv6 and its implications.

As stated previously, the articles of the Directive might be considered applicable to the processing of information derived from the use of IPv6 and, therefore, since the consequences of its use do not differ nor contradict the Directive's principles, obligations, and rights, it would be necessary to determine that there would be no need to modify the Directive.

In this sense, Preliminary Consideration Number 68 of the Directive states that: *'Whereas the principles set out in this Directive regarding the protection of the rights and freedoms of individuals, notably their right to privacy, with regard to the processing of personal data may be supplemented or clarified, in particular, as far as certain sectors are concerned, by specific rules based on those principles'.*

Likewise, the duty of adequacy of these principles to more specific sectors will have to be carried out, for example, by specific legislation or codes of conduct which help, in a dynamical and flexible way, to adapt these principles to every sector involved in the processing of personal data.

Article 27 of the Directive distinguishes between national Codes of Conduct, which will have to be promoted by the Member States and checked by the national authorities on data protection and community Codes of Conduct, which will be submitted to the review of the Article 29 Working Party.

4.2. Directive 2002/58/EC

This Directive is more closely connected with the supposition that is the object of analysis of this publication (implementation of IPv6), since it regulates the specific requirements for processing personal data in relation to the new services of electronic communications. Some of the aspects regulated might be the services of location of terminals, the supply of information, traffic data processing and, in general, any service that could be provided through public electronic communications networks.

In any case, it is important to highlight that what is not regulated by this Directive, will nevertheless be covered by Directive 95/46/EC. For this reason, this section only will consider the specific matters covered by this Directive 2002/58/EC.

4.2.1. Consideration of IP addresses as Traffic Data

One of the most important concepts in this Directive is 'Traffic Data' which is defined in paragraph b) of its article 2.

'Traffic Data' must be understood to mean *'any data processed for the purpose of the conveyance of a communication on an electronic communications network or for the billing thereof'.*

And 'communication' must be understood to mean *'any information exchanged or conveyed between a finite number of parties by means of a publicly available electronic communications service'.*

In this regard, the Preliminary Consideration Number 15 clarifies that *'traffic data may, inter alia, consist of data referring to the routing, duration, time or volume of a communication, to the protocol used, to the location of the terminal equipment of the sender or recipient, to the network on which the communication originates or terminates, to the beginning, end or duration of a connection '.*

As a result, it is possible to consider an IP address as traffic data because it helps to conduct the communications along the network.

In this respect, the Directive introduces some parameters which must be considered in the processing of this kind of personal data.

4.2.1.1. General considerations about Traffic Data

Article 5 of the Directive establishes the need to assure the confidentiality, not only of the information which is transmitted, but also of the traffic data related to this information.

This kind of information should only be intercepted, recorded, stored, listened to or monitored when:

- The user has consented.
- Those who carry out these actions are legally authorized to do so.

Nevertheless, the Directive allows for the technical storage of traffic data when it is necessary for the conveyance of a communication. Therefore, if the storage of this kind of data by the Internet access providers, telecommunications companies, etc, is only for this purpose, it would be allowed by the Directive.

Extrapolating these considerations to IPv6, IP addresses, as traffic data, must be confidential. The fulfilment of this obligation is more important in relation to an IP generated with a Unique Identifier since it would be simpler for a non authorized third party, to associate the communication, with the IP, with the machine and with the user that generates it.

For this reason, it is possible to process this kind of traffic data for the following purposes: The conveyance of the communications, subscriber billing and the interconnection of payments. For processing of this type of information for any other reason (i.e. commercial promotion or provision of value added services), as a general rule, the consent of the data subject will be needed (tacit or explicit).

Finally, it is important that every provider or agent that processes this personal information, in any case, will have to comply with their duties in relation to the information and obtain the required consent, as has been outlined in the previous paragraph.

4.2.1.2. What is the conservation period for Traffic Data?

The Directive allows for the storage of traffic data by certain providers, but it must be done in conformity with a series of criteria that guarantee that the data is stored only for the period of time necessary. In addition, this kind of data must be erased when it has stopped being necessary for the purposes that motivated the processing (the conveyance of the communication). Also, its processing is allowed for some purposes such as subscriber billing and for the interconnection of payments, so it can be concluded that traffic data would have to be erased when its continued storage is not necessary for the fulfilment of these purposes.

Preliminary Consideration Number 27 clarifies that '*the exact moment of the completion of the transmission of a communication, after which traffic data should be erased except for billing purposes, may depend on the type of electronic communications service provided. For instance, for a voice telephony call, the transmission will be completed as soon as either of the users terminates the connection. For electronic mail, the transmission is completed as soon as the addressee collects the message, typically from the server of his service provider'.*

Also, it is significant that one of the alternatives offered by the Directive instead of the erasure of traffic data is to make it anonymous. This possibility raises certain practical difficulties for the providers, in case of the IP addresses generated by a Unique Identifier. These providers would need to adopt some type of measures which make it impossible for them to associate the IP with the user.

Although, these are the main points of the Directive, it is important to highlight a new legislative trend that was being forged within the EU during the preparation of this publication. This trend is based, among other reasons, on the need to fight and prosecute the crimes of terrorism, which could result in series of modifications or amendments regarding the processing and conservation of traffic data.

Specifically, through the press release 7555/04 (Presse 94) of the Extraordinary Session of the Council of Justice and Matters of Interior, held in Brussels on March 19, 2004 as consequence of the terrorist attempts perpetrated in Madrid and presided over by D. Michael

McDowell, the European Commission has demonstrated its intention to present in June 2004, a proposal to force Internet providers and the telecommunication companies to store, (for a minimal period of between 2 and 3 years), the traffic data of the users, with the principal aim to attack, using the Internet as a method to assist the commission of terrorist acts.

This future regulation would not be contradictory with what is established in the present Directive since its article 15 allows the adoption of measures to restrict the scope of the rights and obligations of the users and subscribers, when these restrictions are necessary to protect safety, the investigation and prosecution for the commission of criminal acts.

Nevertheless, it would be necessary to regulate the limitations in the use of this type of information during the term allowed for its conservation.

4.2.2. When does the Directive require the obtaining of the users/subscribers´ consent for the processing of their personal data?

Generally speaking, the scope of the Directive states that any activity related to he provision of services of electronic communications which goes beyond the mere conveyance of a communication or billing the service (i.e. the provision of value added services), will have to be based on anonymous information and, in case this is not possible, it will be necessary to obtain the data subject's consent.

4.2.3. Presentation and restriction of the calling and connected line identification

Another main article that could be applied to IPv6 is article 8, which deals with the presentation and restriction of calling and connected line identification. In this respect, although this article might seem to be more focused on the regulation of the services of telephony (mobile or landline), it may be understood that it could be applied to the different cases of electronic communications carried out by using IPv6.

This article demonstrates the intention of the legislator to preserve the privacy of the user who carries out the call, obliging the service provider to offer him technical possibilities that avoid the identification of the calling line, when there exist the possibility that this could be visualized.

In the same way, the legislator wishes to protect the interests of the user allowing him, when receiving calls, to reject the incoming calls when the identification of the incoming caller has been prevented by the calling user.

Following the criteria established in this article, it could be said that, regarding the IP addresses based on a Unique Identifier, users must be able to demand of their providers the adoption of certain preventative mechanisms:

- The identification of the IP address of the user, in the cases in which this identification is not necessary.

- The possibility for the recipient to reject communications transmitted with a certain IP address, when the sender uses the option which allows the restriction of the identification of his IP.

Nevertheless, the Preliminary Consideration Number 19 states that, in those particular cases in which the adoption of these measures is technically impossible for the providers or in which it requires a disproportionate economic effort, the implementation of these measures will not be mandatory. In any case, the interested parties will have to be informed of this impossibility and the Member States will have to notify them to the Commission.

In certain ways, at present, some technical measures are being adopted that encourage these types of activities which are applicable to the IP addresses, some of them based, actually, on the proposed standard RFC3041.

However, the Directive sets out several cases in which the provider might override the restriction of the identification of the incoming caller. These cases are:

- When it is necessary to trace malicious or nuisance calls.
- When it is necessary to deal with emergency calls, by organizations recognized by the Member States such as enforcement agencies, ambulance services, fire brigades, etc.

4.2.4. Consideration of IP addresses as Location Data

'Location Data' must be understood to mean, as it is stated in article 2 c) of the Directive *'any data processed in an electronic communications network, indicating the geographic position of the terminal equipment of a user of a publicly available electronic communications service'.*

In conformity with the Preliminary Considering Number 14, the location data will be that referring to *'the latitude, longitude and altitude of the user's terminal equipment, to the direction of travel, to the level of accuracy of the location information, to the identification of the network cell in which the terminal equipment is located at a certain point in time or to the time the location information was recorded '*.

In mobile digital networks, it is possible to process location data (which are considered to be traffic data) which can provide the geographic position of the terminal equipment of the mobile user to enable the transmission of the communications.

This fact takes on significant relevancy in the cases in which a device with mobility (PDA's, laptops, mobile telephones, etc.) accesses the Net using an IP, since apart from the existence of the possibility of tracing its movements and surfing, it would be possible to know its physical location, both of the terminal and of the owner of that terminal.

This possibility enables different types of new processing of information that will have to be regularized in conformity with the Directive 95/46/EC and the national legislation of the

Member States, for example, the possibility of acquiring (in most of the cases in an illicit way) this type of information for providers of services of information about the conditions of the vehicles traffic, to offer certain services to a user, on occasions without his specific request (i.e. the state of the traffic in the highway along which he is driving); the control of the teleworkers or the creation of profiles, habits of a certain person, which, from a merely commercial aspect, might bring important economic advantages for those who want to take advantage of these types of technological advances.

In this respect, it is important to highlight that the Directive establishes that this type of information, will only be able to be processed with the consent of the user and, although this have been given for a specific moment, there must be established mechanisms that enable the withdrawal of this consent at any moment.

Likewise, the Directive allows for the processing of this kind of information, by those agents who act in the name and under the instructions of the electronic communications services provider, acquired by the user, not allowing to non authorized third parties to process them.

4.2.5. Regulation for the guides of subscribers

As will be considered in later sections, one of the means that would allow the association of a certain IP with a certain user and, therefore, that would promote the consideration of the information of IP as personal data, is the adoption of public guides which contain the description of the user and his IP address.

Taking this into consideration, it might be useful to have in mind the criteria established by the Directive regarding this type of public guides.

The user can decide if he wants to disclose his personal information to a third party or not, but, in any case, the incorporation of this data in the abovementioned guides will require that the entities in charge of their provision or the service providers regarding these guides, inform the owners of the information kept of the purposes of these guides, as well as of the rest of the parameters of the duty of information (transfers of information, possibility of exercising the rights of access, rectification, etc.), and obtain their consent.

In this respect, any use of these guides by an agent based on different purposes as those for which the consent was obtained initially from the data subject, will require the obtaining of a new consent by this agent.

In short, article 12 establishes a series of parameters that will have to be born in mind by the Member States at the time that these public guides are created:

- Obligation to inform the owners of the information (subscribers) of its incorporation in the guide.

- Possibility that the guides are printed or electronic.
- Subscribers' power to decide, which data are going to appear in the guides.
- Respect for the main principles and obligations of this legislation, in terms of the quality of information: incorporation of suitable, pertinent and not excessive information.
- The fact of not being included in this kind of directories or any other activity related to these must be free of charge.

The analysis of the consequences that the creation of this type of IP guides might bring is set out in section. 5.3.1. of this chapter.

4.2.6. Must the Directive 2002/58/EC be modified because of IPv6?

At the moment, this Directive is the regulatory framework for privacy and data protection which comes closest to the regulation that should be offered because of the use of the new Internet Protocol version 6.

Most of the articles gathered in the Directive regulate some cases that, directly or indirectly, could be related to IPv6. In certain cases, like the possibility of restricting the identification of the line of origin or the regulation of the public guides of subscribers, although it seems to be clear that the above mentioned articles try to regulate different cases, they might be applied analogically to the use of the Protocol in its new version 6.

In this respect, it could said that this Directive offers the general criteria to be taken into consideration by the Member States at the time of regulating the use of IPv6 by each of their domestic legislations and the way of complying with the obligations imposed by this Directive and the Directive 95/46/EC.

4.3. Normative Developments on Data Protection Adopted by the Member States

As a consequence of Preliminary Consideration number 22 and of article 32 of the Directive 95/46/EC, the Member States will have to adapt their national legislation in accordance with the regulations contained in this Directive. For this reason, the different Member States have passed their own laws in order to regulate these matters.

For information purposes, some of these States that already have regulation, more or less restrictive, on data protection are Germany, Austria, Belgium, Denmark, Spain, Finland, France, Great Britain, Greece, Holland, Ireland, Italy, Luxembourg, Portugal and Sweden.

As will be seen below, country by country, there are not many innovations contained in these regulations, which are usually a mere reflection of the dispositions of the above-mentioned Directive 95/46/EC.

Since it has been introduced, the main laws approved by the Member States on data protection replicate faithfully the obligations, rights and principles stated in the Directive 95/46/EC, so it is not common to find 'new' applicable articles intended to regulate specific cases like IPv6. In this respect, it would be necessary to analyze the legislation adopted by these States, which intend to legislate some specific sectors of activity as, for example, the telecommunication or Internet sectors.

4.3.1. Germany

Germany was a pioneering country in the adoption of data protection regulation, since the first law was that known as Law of Hesse, of October 7, 1970.

Later, it was passed as the German Federal Law on Data Protection January 27, 1977, which was subsequently amended by the law called Bundesdatenschutzgesetz (BDSG), which came into force on June 1, 1991.

The regulation that is currently in force is the named 'The Federal Data Protection Act' (Bundesdatenschutzgesetz) of May 18, 2001.

Likewise, it is important to emphasize that several laws have been approved by different German cities (Berlin, Brandenburgo, Essen, Saarland, etc.) on this matter.

4.3.1.1. Main aspects

The objective of the Act is to protect the individual against his right to privacy being violated through the processing of his personal data (article 1). For this purpose, the norm is a true reflection of the personal data protection model created by the Directive 95/46/EC and regulates principles and obligations, such as the quality requirements in the collection of data; need of obtaining the consent for the processing; safety and audit principle, etc.

Likewise, in Chapter III, functioning of the German Authority of Control (Federal Data Protection Commissioner) is regulated.

4.3.2. Austria

The first Austrian law on data protection (Datenschutzgesetz) is dated October 18, 1978 and this was amended later by the Decision 609/1989 of the Constitutional Court.

The current Act in force is the Federal Act Concerning the Protection of Personal Data (Dasenschutzgesetz 2000), which came into force on January 1, 2000.

Personal Data Protection

Likewise, different regions (Länders) have adopted their own regulation, such as Kärnten, Salzburg or Vienna, among others.

4.3.2.1. Main aspects

Some of the most important aspects contained in this Act are the following:

The right to data protection is considered to be a fundamental right (article 1).

The restrictions on the right to secrecy are only permitted to safeguard the overriding legitimate interests of another (article 1).

The controllers of a joint information system (joint data processing system by several responsible persons with reciprocal access to the data) shall, unless already regulated by law, appoint a suitable operator for the system, whose name and address shall be included in the notification for registration in the Data Protection Register (article 50).

In short, apart from adapting the Directive 95/46/EC, the Austrian law regulates, in the framework of this Directive, some issues that do not appear in other legal systems, like that mentioned article 50.

4.3.3. Belgium

The first Law on data protection adopted in Belgium is dated December 8, 1992. The current regulation came into force on September 1, 2001.

4.3.3.1. Main aspects

The law states that every individual has the right to the protection of his liberties and fundamental rights, particularly to the protection of his private life in relation to the personal data processing (article 2).

The law applies to automatic processing as well as to non-automatic (article 3). Following this initial policy, the law determines the requirements established by Directive 95/46/EC and, therefore, sets out some of the main principles and obligations such as the obligation to register files; to respect the rights of the data subject; the special processing of the sensitive data, etc.

4.3.4. Denmark

In Denmark, the first legislation on data protection was two-fold: One applicable to files in public ownership, the Law 294 of June 8, 1978 on public records (later modified on several occasions) and another for files in private ownership, the Law 293 of June 8, 1978 on private records, also modified on several occasions.

The current legislation in this matter is 'The Act on Processing of Personal Data' (Act No 429) of May 31, 2000.

4.3.4.1. Main aspects

The Act applies to data processing, automatic or not, where the data subjects are individuals. Nevertheless, certain parts apply, as well, to data processing relating to companies (article 1), so a significant change is introduced in comparison to the application and scope contained in Directive 95/46/EC.

The Act states that Official authorities and private companies may not carry out any automatic registration of the telephone numbers from which calls are made, except with the prior authorization from the supervisory authority in cases where important private or public interests permit. This prohibition shall not apply when it is carried out by operators of telecommunications or in the rendering of services for the identification of the lines.

4.3.5. Spain

In Spain, the first law that came into force was known as LORTAD, Organic Law 5/1992, of October 29, containing the regulation of the automated personal data processing.

Later, this law was repealed by the Organic Law 15/1999 of December 13, of Protection of Information of Personal Character (also known as LOPD), currently in force.

Similarly, it is important to understand that article 9 of the LOPD was developed by the Royal Decree 994/1999, 11th June, the Regulation of Security Measures to be adopted in personal data processing. This Regulation determines the appropriate technical and organizational security measures to be adopted in order to maintain security and to prevent any unauthorized processing of personal data.

In this sense, this Regulation determines three different personal data categories or security levels (basic, medium or high security levels). Each level includes different security measures which must be implemented depending on the type of personal data to be processed.

4.3.5.1. Main aspects

The objective of the law is to guarantee and protect, regarding the personal data processing, the public freedoms and the fundamental rights of the individuals and, especially, of their honor as well as personal and family privacy. In general terms, the Spanish Law is a true reflection of the common community regime established by the Directive 95/46/EC. In this respect, it regulates the principle of quality of data; duty of information; need to obtain the consent for the processing (in general); special processing of sensitive data; conditions for data processing carried out by third parties, etc.

Some of the articles that might be related to some of the topics to be studied in this publication are the ones concerning the phone directories that are considered to be a source accessible to the public, in the terms contained in their specific regulation.

Personal Data Protection

4.3.6. Finland

The Finnish regulation on personal data has been based on three fundamental laws:

Law of April 30, 1987 on files of personal information.

Law of April 30, 1987 on the Commission and the Ombudsman for the protection of information.

Decree of April 30, 1987 on files of personal information.

Now, the legislation in force is 'The Finnish Personal Data Protection Act' (523/1999) of April 22. Nevertheless, this law has suffered certain modifications made by 'Act on the amendment of the Personal Data Act' (986/2000) that came into force on December 1, 2000.

4.3.6.1. Main aspects

Article 1 establishes that its aim is to implement, in the processing of personal data, the protection of private life and the other basic rights that safeguard the right to privacy, as well as to promote the development of and compliance with good processing practice.

Some of the general rules for the processing of personal data, which are set out in Chapter 2 of the rule, are: the determination of the purpose of the processing; the obligation to process personal data exclusively in conformity with the above mentioned purpose; the quality of the information; the duty of information; the processing of sensitive information, which is prohibited if there do not happen some of the circumstances pointed out in the article, such as the obtaining of the express consent of the data subject; international transfers; the regulation of the rights of access and rectification, etc.

One of the innovations set out on Section 13 relates to the processing of the identity personal number. This processing needs to be based in the obtaining of the unequivocal consent of the data subject.

In the same way, Section 17 regulates the creation of public registers. Personal data can only be included in these public registers if the data subject does not prohibit the collection and introduction of that data in those registers.

Another innovation found in this rule is in Section 21, which establishes different periods of keeping of the information by the controllers of the files containing personal data.

Finally, under Section 38 the Authority of Control on data protection in Finland, called The Data Protection Ombudsman, is created.

4.3.7. France

The first French law on this matter was the Law 78-17 of January 6, 1978. Nowadays, the French Parliament is debating the adoption of a series of modifications to this law.

4.3.7.1. Main aspects

Article 1 state that the processing of personal data will not infringe human identity, neither the rights of the individual, nor privacy, nor individual or public freedoms.

The concept of automatic processing of personal data refers to any series of operations effected by automatic means, including the collection, recording, preparation, modification, storage and destruction of personal data, as well as any operations relating to the use of files or data bases, including interconnections, the consultation or the communication of personal data.

Since the French law predates Directive 95/46/EC, it is necessary to guarantee its evolution in conformity with the criteria indicated by the Directive and, therefore, these criteria will have to be born in mind for the new regulation that will be adopted in France.

4.3.8. Great Britain

The British legislation on data protection begins with the Law of July 12, 1984 (Data Protection Act). Likewise, Great Britain has a Regulation, October 13, 1985 dedicated to the Data Protection Court.

Later, this legislation has been repealed, being in effect 'The Data Protection Act of 1998'.

4.3.8.1. Main aspects

Through this regulation, different obligations required by Directive 95/46/EC are regulated. In Chapter I, some of them are set out such as the right of information, obligation to rectify, block, erase or destroy personal data, prohibition of processing personal data if, previously, the file has not been notified to the British Authority of Control called 'Data Protection Commissioner '.

Likewise, it is stated that any processing of information that is carried out for the purposes of prevention or detection of crimes, arrest or prosecution of the persons in charge, will not be linked to the duty of information. In this sense, the processing of IP address data according to these purposes will not require the compliance by the controller, with the information duty.

The principle of obtaining the consent as a main requirement to effect a processing or transfer of personal data is set out in Section 55.

Part II of the statute, sets out the interpretation of the principles contained in the statute as well as the determination of the conditions to be born in mind for the processing of all kinds of information and, specially, of sensitive information, as well as determine the cases in which each of these principles would not be applied.

Personal Data Protection

4.3.9. Greece

The Greek Law 2472/1997, on protection of individuals with regard to the processing of personal data was approved on April 10 of 1997.

4.3.9.1. Main aspects

The scope of this law is to determine the conditions regarding the processing of personal data and the protection of the human rights, fundamental freedoms and private life, as it is established in article 1.

Following the guidelines of Directive 95/46/EC, this law is outlined with respect to certain principles such as the quality of the information, the duty of information, the need to obtain the consent for the processing of personal data, except in those cases considered as exceptions in article 2. In any case, it will be necessary to obtain written consent for the processing of sensitive data.

Other principles and obligations relate to the interconnection of files, which will have to be reported to the Greek Data Protection Authority and, in case they should be based on sensitive information, the controller would have to obtain prior authorization, the regulation of international data transfers; the exercise of the rights of access and opposition or sanctions and penal and administrative infringements, among others.

4.3.10. Holland

The first Dutch law on data protection was the Law of December 28, 1988, called 'Wet Personenregistraties' and better known as WPR.

Nowadays, the regulation in force is the 'Personal Data Protection Act of July 6, 2000'.

4.3.10.1. Main aspects

This law applies to the automatic processing of personal data, as well as to non automatic processing.

Articles 7 to 11 set out some of the requirements that must exist in any processing of information: the obtaining of information for legitimate, specific and explicit purposes; data must be necessary for the fulfillment of a legal obligation or for the fulfillment of a contract (among other reasons); conservation of the information during the time necessary for the fulfillment of the purpose of processing, etc.

On the other hand, articles 16 to 24 regulate the processing of the sensitive information (religion, philosophy of life, politics, race, health, sexual life, trade union membership and criminal behavior).

In some cases, for example, for the processing of information regarding race or ethical origin, amongst the reasons that allow its processing, it is the fact that the data subject had not refused this processing in writing, which differs from the regulations of other Member States on this matter.

Article 25 sets out the possibility of the adoption Codes of Conduct by different entities, for which the approval of the Data Protection Commission (Dutch Control Authority) would be needed.

The duty of information is set out in articles 33 and 34 of this law. Likewise, this law also regulates the rights of data subjects, the international transfers and the breaches and sanctions, among other obligations already imposed by Directive 95/46/EC.

4.3.11. Ireland

The first Irish Law on data protection was dated July 13, 1988. Now, a Bill of law is being debated before the Parliament.

4.3.11.1. Main aspects

The Data Protection Act of 1988 is a quite old law. Article 1 defines 'personal data' as all information relating to a living individual who can be identified either from the data or from the data in conjunction with other information in possession of the data controller.

Articles 4 to 6 regulate the conditions for the exercise of the right of access and rectification by the data subjects.

The Irish Control Authority (called the Commission) is created by articles 9 and 10.

Other common matters regulated by this law are the international transfers of personal data; the specific requirements for the notification of files or breaches and sanctions.

4.3.12. Italy

The Italian Law on data protection is the Law 675/96 of December 31 (Tutella delle persone e di altri soggetti rispetto al trattamento dei dati personali). In addition, a set of laws has been approved on the basis of this statute, especially, royal decrees such as: nº 123 dated May, 1997; nº255 dated July, 1997; nº135 dated May, 1998 or the most recent, nº 282 dated July, 1999.

4.3.12.1. Main aspects

As established in its article 1, this law tries to assure that the processing of personal data is carried out respecting the fundamental rights and freedoms and the dignity of natural persons, with special regard to their right to privacy.

Similarly, as an innovation, it guarantees the rights of legal bodies, in this respect.

Personal Data Protection

Following the criteria of Directive 95/46/EC, some of the main principles are: data quality; the duty of information to be given while collecting personal data; the obtaining of the consent and exceptions; data processing security, principles that will be implemented by a royal decree; data disclosure to third parties; the processing of sensitive information or international transfers, among others.

Specifically, this law sets out what must be done by the controller of the file, as soon as he finishes the processing of personal data: to destroy them, to transmit them to another person in charge or to be stored separately.

4.3.13. Luxembourg

The first existing regulation on data protection in Luxembourg were the Law of March 31, 1979 (Act Regulating the Use of National Data in Data Processing), which has undergone several modifications and the Grand Ducal Regulation of August 2, 1979, on the Council of State created by article 30 of the law of March 31.

At the moment, the present law in force came into effect in 2002.

4.3.13.1. Main aspects

The law protects the fundamental rights and freedoms of individuals, especially in their private lives, in relation to their personal data processing.

In conformity with the definition of 'Processing of personal data' set out article 2, the law applies to the automatic and non automatic processing of personal data.

As we can see, a clear trend can be observed regarding the faithful transposition of regulation on data protection established by Directive 95/46/EC.

4.3.14. Portugal

The first Portuguese law on data protection is dated April 9th, 1991 (Law 10/91). Currently, the Law in force is Law 67/98 of October 26 (Lei da Proteccao de Dados Pessoais).

4.3.14.1. Main aspects

The general principle of this law is set out in its article 2: personal data processing must be carried out in an open way and have respect for private life, rights, freedoms and fundamental guarantees.

This law does not introduce innovations regarding the principles and obligations imposed by the Directive 95/46/EC, which are: data quality; the need to obtain, generally, the consent of the data subject to be able to process his personal data; special conditions for the processing sensitive data; the regulation of the interconnection of data; the rights of the data

subjects; duty of information; security measures; the processing of personal data by third entities; international data transfers; codes of conduct; etc.

The controlling authority in Portugal is called the Proteccao's Comissao Nacional de Dados, also known as CNPD.

4.3.15. Sweden

The first Swedish law on data protection was the Law 1973/289 that was later modified in 1989. At present, the law in force is the Personal Data Act (1998/204).

4.3.15.1. Main aspects

The scope of this law is to protect individuals against the violation of their personal integrity by the processing of personal data.

As with the rest of the national regulations which have been considered, this protection is ensured by a series of principles and obligations which should be adopted by those who process personal data.

This Law establishes a few essential requirements to bear in mind regarding any personal data processing: The legitimacy of the processing; clear determination of the purposes of the processing; the need for adequate, necessary, pertinent and accurate information; general obligation to obtain the consent of the data subject (except in some cases considered as exceptions); special measures to be adopted in the processing of sensitive information; duty of information; regulation of processing carried out by a third party, etc.

5. Practical Problems

Having analyzed the current data protection legislation adopted by the Member States, there follows in this section, an explanation of some of the practical problems with implications for data protection regarding the implementation of IPv6.

5.1. New Processing of Personal Data as Consequence of the Use of IPv6

The IP address may be considered as personal data if the possibility exists of relating that IP address (based on the Unique Identifier which may be part of it) to the interface of the terminal accessing to the Net and, in consequence, if there may also exist the possibility of relating that data to the user or owner of that IP.

This fact has two consequences that, necessarily, would have to be regulated:

- The consequences derived from the obtaining and processing of the IP address based on a Unique Identifier, as personal data itself.

- The new processing of information that could be generated as consequence of the possibility of associating certain information (which until now it was in general perceived as anonymous), different from the IP address itself, with a certain individual. For example, with IP addresses assigned dynamically by an Internet access provider and used with the current Protocol, version 4 a user whenever he was accessing the Net was doing it with a different IP each time he was accessing. In each session, he might access a specific web page where a series of personal data could be requested to him, with the purpose of knowing what type of users access the above mentioned web page, for example, his age and sex.

  In this case, if the user was not providing his name and surname and if the web page did not have mechanisms of tracing, cookies, sniffing software, etc., normally, the above mentioned information would be anonymous. At most, the owner of the web page would be able to associate this information to a specific IP address, which could change every time the user changes his connection to the Net.

  On the other hand, is important to say that still many access providers provide static addresses to the users, and in general because the need of lawful interception and logging of transactions, there is not a real situation of anonymous connection.

On the contrary, with IPv6 this information would be associated with a certain IP based on a Unique Identifier, which would identify automatically the interface of the terminal and, potentially, the concrete user of that IP.

For this reason, the implementation of IPv6 means that both cases imply a processing of new personal data and, therefore, there are new obligations to be complied with by the involved agents that process those personal data.

Is key to remind the importance on this regards of RFC3041, as earlier explained, which provides, when used, a further degree of privacy, not available with IPv4.

5.2. Obtaining Information about IP Addresses by the Processing Agents

One of the examples in which the IP address is considered to be personal data, is when its processing is done by the Internet access providers or by the telecommunications companies.

In this way, these agents enter into a contract with the users of their services. In general, as a consequence of these contracts, these agents could include in their files the IP addresses of their users, other types of information that could be requested in these contracts, such as their names, addresses or bank accounts.

Similarly, these agents could be able to register the date of access to the Net, the time and the duration of the connection.

For this reason, it is important to confirm that, in this case, the contract becomes the link across which the provider associates the IP address with its holder, which brings in a series of obligations on data protection for these providers such as: his consideration as the controller of the files created with this information as consequence of its processing and storage, the obligation to notify and register those files to his national authority on data protection, as well as the fulfillment of the rest of obligations that have been outlined previously in this Book.

5.3. Means to Consider an IP Address as Personal Data

5.3.1. The use of public guides or directories

There are some assumptions for which, potentially, an agent could provide the requested service without needing to know the identity of the user who is behind a certain IP address.

In these cases, although the agent, provider of the above mentioned service, holds the information about this IP address, if he does not have the possibility, by any means, of connecting this information with any other concerning its holder, there would not be a personal data processing and, therefore, this processing would not be governed by this regulation, since the mere information of an IP address would not identify the concrete natural person, holder of the IP address.

Though these arguments are valid enough from a theoretical perspective, let's imagine that, as they exist nowadays for landline telephony, for IPv6, public guides or lists have been created in the style of the Whois Database (accessible to everybody) in which there were set out the names and surnames of the users together with the part of the Unique Identifier that would compose their IP addresses and to which there could have access any agent, for example, holders of web pages or of commercial establishments on the Internet.

The mere fact that there exists the possibility of a third party comparing an IP address with a list and getting to know who the holder is would, automatically, turn this Unique Identifier of an IP address into personal data.

In this case, it is important to highlight that this possibility is related to the creation of public directories containing the Unique Identifier of the different IP Addresses, linked to their holder and not the whole IP address, because there are cases regarding mobile terminals or nodes in which their IP addresses will never be totally the same because some parts of them would change depending on the point at which the connection to the Net is made. On the other hand, those terminals or nodes without mobility that access the Net always using the same point of connection will have the same IP address.

Next, we will be set out a series of considerations regarding the creation of public guides, bearing in mind, among other facts, the considerations established in the Directive 2002/58.

Personal Data Protection

In this respect, it is important to state that the provisions of this Directive relating to subscriber guides are directly focused on the directories generated for telephony, by which it is possible to associate a certain person to his phone number.

In this respect, apart from the differences that this type of public phone directory could have in comparison with those that could be created for IP addresses based on a Unique Identifier, in this section a brief analysis will be made of the regulations offered by the abovementioned Directive regarding this type of public guide.

5.3.1.1. Nature of public directories

One of the first differences that might arise in relation to the type of guides regulated by this Directive is based on the specific nature of the guides or IP address directories that may be produced.

Specifically, the extraterritorial character of the Internet would strongly associate these directories with this extraterritorial nature. Therefore, it could be asked whether there would be a single directory used world wide or, on the other hand, these guides will have a European or national nature. In this respect, it would become important to ascertain the current system of assignment of IP addresses and, initially, it seems likely it will not suffer substantial changes caused because of the use of IPv6, then perhaps this kind of directory could have a world wide nature.

For this reason, the IP guides which are created might have similarities to certain types of currently used guides, which allow us to carry out enquiries using the Internet and to know, for example, from the domain name of an authority, entity or natural person, who has registered it or its DNS server, amongst other information.

In other ways, these guides allow a reverse association, that is, through an IP address, it is possible to recognize what person or entity has registered that identified domain name.

Finally, among the problems derived from the nature of these public directories, another matter that should be born in mind, is the fact that if the production of these directories would be carried out under a system of free and open competition or, on the contrary, it may be decided that their creation should be performed by only one body that would be in charge of its management, its updating and processing, in compliance with what it is required under the data protection regulation.

5.3.1.2. Incorporation of information in the public directories

Firstly, Directive 2002/58/EC is the data protection regulation that sets out the regulation of public guides which, though it does not try to regulate the IP directories who might be generated in the future, it ought to be taken into consideration in this present analysis.

After analyzing the method of incorporation of information into these guides which is established in the Directive, it could be deduced that this simply enables the data subject to decide if he wishes or not to be included in these directories. For this, there could exist two different ways to proceed to incorporate his information in the directories:

- Automatic incorporation of the information in the guide, complying with the duty of information and obtaining of proper consent, so that if the user does not want to appear in the same one, he must request to be taken out of the directory or,
- Specific request of incorporation in the directory received from the user.

5.3.1.3. Some assumptions to be regulated

The creation of this type of directory would suppose the generation of a series of cases that have to be regulated according to the data protection legislation. These cases, likewise, would be influenced by the system of allotment of IP addresses and, therefore, by the entities empowered to create lists with the users and their respective IP addresses (the Unique Identifier part of the IP´s).

Another important matter would be the way of adding to and updating these guides that, in occasions, would be based on the transmission of the information to be included in them, from the agents with the capacity to allocate IP addresses to the users, to the entity or entities in charge of their production.

Likewise, there should be regulation of the position of this entity or entities and the ownership of the files generated from the creation of these guides.

Specifically, who would be considered the controller of the data contained in these guides: The entity or entities that generate them or the operators or providers who obtain such information and supply it to that entity/entities?. This will be one of the questions for debate in the event that these guides are adopted. This question is not a trivial one because depending on what entity or entities would be considered as the controller of such files, it would be possible to know which of them will have to comply with the duties of information, obtaining of the consent for the incorporation of the information in the guides, etc.

Similarly, if it were decided that these managing entities should not be created but the agents who process this information and allocate IP addresses are enabled to produce their own directories, it would be them who, in any event, should inform the data subjects about the incorporation of their personal data in the abovementioned directories, the purposes of the processing of their data, as well as complying with the remaining matters such as the obtaining of consent, etc.

On the other hand, there should also be data protection obligations in existence for other agents who use and process the information contained in these directories. That is, for example, those agents that, though they would not take part in the production and/or updating of the information contained in the guides, may use them to associate IP addresses based on a Unique Identifier with a certain user, or holder of the concrete IP.

5.3.1.4. The use of Reverse Directories

The revolution in new technologies and the digitalization of information has enabled the development of new possibilities for accessing the information contained in public directories, which make it easier to associate personal information with other types of information.

In this regard, there are some types of directories which make it possible to search for information in a reverse way. In this way, there are reverse directories or multi-criteria directories that enable us, by means of a phone number, to obtain personal information about its holder (name and surnames, address, etc.). Another example are the guides, generally consulted in the Internet, which enable us to obtain certain information about the entity or natural person who has registered a domain name, by the simple provision of that domain name.

Because of the similarity of this type of guide with the ones that should be created in the near future regarding IP addresses (through the IP one might obtain information about its holder), it would be important to bear in mind the following considerations.

These practices of reverse searching have originated and given rise to important concerns, at least, regarding the use of reverse phone directories, based on the possibility of invading the right to privacy and data protection which belongs to the data subjects. This concern has produced that some domestic legislation, especially telecommunications regulations, which have resulted in the prohibition of their use or have set down a series of requirements for their creation, on the basis of the recommendations carried out by the Opinion 5/2000 on the Use of public directories for reverse or Multi-Criteria Searching Services, adopted on July 13, 2000 by the Article 29 Data Protection Working Party.

This Opinion admits that, in many cases, this type of directory can be contrary to the privacy of the users, because it is understood that use of these public guides based on the purpose of verifying personal information concerning the holder of the phone number, constitutes a totally different use from the one which motivated the data subject to give his consent to provide his personal data for use in a public directory.

Nevertheless, it states that, in other situations, they could be useful and, therefore, they should not always be prohibited, but it is necessary to adopt all the measures set down in the Directive 95/46/EC to enable the regulation of: Duty of information and obtaining of consent from the data subject, among other obligations.

Therefore, it is important to take these points into account and bear in mind the differences outlined above between reverse phone directories and those which might be created in relation to IP addresses. Therefore, it is possible to conclude that, although the general rule is the option of not producing and using these directories, in the cases in which they could be considered to be really useful, it would be necessary to comply with all the existing principles and obligations on data protection, specially, the duty of information and obtaining of the consent of the data subjects for the inclusion in the guide of their personal data and their subsequent processing in conformity with the established purposes.

5.3.2. Contracting of services

Although the creation of public guides with lists of IP addresses is one of the methods used to relate an IP to his holder, there are other ways that could be used to associate this type of information with its holder and, therefore, that could turn this type of data into personal data.

For certain agents, when the user is contracting a service, it is a fundamental requirement to obtain the IP address based on the Unique Identifier to be able to provide the service correctly. For example, let us think about an Internet access provider. In this case, this agent would associate an IP address with its holder through the contract.

Another example, regards the possibility that household appliances could incorporate IP addresses based on a Unique Identifier. This raises the possibility that, for example, supermarkets could begin to provide some services based on sending the products which were demanded by a fridge, as soon as it had detected the lack of the product.

In such cases, it could be the case that the provider of this service could need to associate the IP address with, at least, the address to which it must send the ordered product and, therefore, with its holder who will have to pay for the service.

In these cases, the normal method of obtaining this information would be from signing the contract with the user.

For this reason, in relation to the providers of these services, it could be understood that the information of the IP address would be considered as personal data since the association of the IP address with its holder, would be achieved by these providers through the contract entered into by them.

In this case, the contract is the most suitable means to be used by this kind of service providers or agents to comply their information duties as well as the obtaining of the data subject's consent to process their personal data.

Personal Data Protection

5.4. Possibility of Maintaining IP Addresses based on an Unique Identifier

Another legal problem that might arise is based on who or what entity will be in charge of allocating these types of IP addresses and, likewise, in case they are granted by the Internet access providers or by the telecommunications companies, if those IP addresses are intended to be the same for every user or they would be changed, instead, when a user changes his access provider or telecommunications company.

The fact that these addresses would not be considered 'permanent' for each of the users could bring about the need to carry out certain relevant activities, which should be regulated.

For example, the obligation to update the public directories that might be generated and the requirement that access providers, telecommunications companies and any other agent that processes this kind of data, communicates any modifications undertaken regarding these IP addresses.

In these cases, it would be useful to develop some regulations that help to determine the criteria to be born in mind relating to the processing of this information, in conformity with the data protection legislation then in force.

5.5. Possibility of Tracing the User's Activities

One of the main problems that have been detected with regard to the implementation of the IP addresses based on a Unique Identifier, is the fact that it is possible to trace the activities being carried out by the user connected to the Net (which already was possible in the version 4 of the Protocol by using cookies or spy programs), but the innovation is based on the fact that the results of the tracing can be associated to a given interface in a terminal and, potentially, to its holder.

Normally, the users are unaware that while they are surfing the Net, typing an URL or downloading something, their browser will systematically transmit their IP address based in a Unique Identifier. In these cases, their personal data could be collected and further processed for purposes that are unknown to them.

Since one of the principal features of the regulations we have analyzed is that the processing of personal data must be carried out with some guarantees for the data subject, this possibility allowed by IPv6 favours new types of personal data processing that, till now, did not need to be regulated.

For example, an eavesdropper would be able to link this information with its holder, being able to find out, for example, the places or web pages visited by the user, his connection

and disconnection hours, the products or services acquired, the purchases carried out, for example, through the requests effected to the supermarket by his fridge, and even, the location of the terminal from which the corresponding communications are being carried out.

Nevertheless, analyzing these cases from another perspective, may be less alarmist, it is possible to realize that at the moment in which a user obtains a certain IP address based on a Unique Identifier, he should begin to be conscious of the possibility that this type of processing can be carried out with his personal data and, also, he might be informed of this by the different agents that are going to process his data. As a result, these agents must be obliged to provide the users with some technical measures that guarantee the preservation of their privacy while accessing and surfing the Net (i.e. RFC3041).

In this respect, the Common Position regarding Online profiles on the Internet adopted at the 27th meeting of the Working Group on 4/5 May, 2000 in Rethymnon, Crete, establishes for Internet service providers the obligation to notify users, in any case, the type, scope, place, duration of storage and purposes of collection, processing and use of their data for profiling purposes.

Also, this obligation to inform must be complied with even in the case of data being collected using pseudonymous.

5.6. What Means can exist to Comply with the Duty of Information by the Personal Data Processing Agencies?

In some senses, it could be stated that IPv6 does not introduce different problems for the compliance with the duty of information by the agents, which process personal data that did not exist with previous versions of the Protocol.

In the cases in which a contract is entered into by the user and the agent or provider which tries to keep his IP address for certain processing purposes, an informative clause should be included in the aforementioned contract.

On the other hand, if the above mentioned obtaining and processing of personal data is affected through the use of any service provided in the Internet, by using any terminal or device connected to the Net, the agent or provider who processes this data must include the informative clause in each of the accesses web pages.

In this respect, it is important to highlight that if a certain agent had informed the holder of the IP address about each one of the aspects determined by the Directive regarding the information duties, included the purposes of the processing of his personal data, in case that at a later date, he decides to process them for different or new purposes, he would have to inform the data subjects, once again, of this intention as well as to obtain their due consent (tacit in a few occasions and express in others) for the processing of the data according to these new purposes.

In short, as regards the fulfilment of this obligation, as well as some of the others contained in the current legislation on data protection, there are no specifics concerning the way to comply this obligation. Maybe, the main change derived from the implementation of IPv6 relates to the fact that there will be more agents who must comply their information duties because, with IPv6, more information might be considered as personal data.

5.7. Mobility in IPv6

The term 'mobility in IPv6' refers to all those mobile devices that have the possibility of being connected to the Net at different points, so it seems that they are 'moving along the Net' (i.e. laptops, mobile phones, PDA's, etc).

It is a question of asking whether any device can be connected at one point or another of the Net without losing its IP address. Therefore, mobileIPv6 allows a mobile node to move from one link to another without changing the mobile node's IP address.

Let's think about an executive's laptop, which can be connected to the Net from his office, house, from the hotel where he stays, etc.

For this type of device, it could be questioned whether its IP addresses, based in IPv6, contains the part of the Unique Identifier and, therefore, the possibility exists of identifying these devices and, potentially, their holders.

In this case, if it is possible that this type of IP addresses is given to mobile devices, how is it then possible to identify them if these devices can be connected to the Net from different physical places, bearing in mind that when these devices move along the Net, they generate new IP addresses as consequence of their new point of connection?.

At the same time, it is important to highlight that although a part of the IP address is being modified depending on the connection point, the Unique Identifier contained in the IP address does not suffer any modifications. Thus, it is possible to identify these devices.

However, this possibility raises problems beyond the mere identification of the user, for example, the possibility of knowing his geographical location. An IP address could be considered as location data as it is stated in section 4.2.4.

In addition, since location data are considered as traffic data, telecommunication operators and ISPs have the obligation of retaining those data in order to help with the prosecution of illegal activities. In these cases, although the privacy of the users seems to be affected, the user may have in mind that this retention of their data is a processing imposed by the law in force and that their capacity to restrict this processing is clearly reduced.

In this sense, Directive 2002/58/EC allows the Member States to determine what means will be used for the retention of traffic data. Thus, its article 15 establishes that 'Member

States may adopt legislative measures to restrict the scope of the rights and obligations provided for in Article 5 (Confidentiality of the communications) and Article 6 (Traffic Data), Article 8, section 1, 2, 3, 4 (Presentation and restriction of the calling and connected line identification) and Article 9 (Location Data), when such restriction constitutes a necessary, appropriate and proportionate measure within a democratic society to (...) prevention, investigation, detection and prosecution of criminal offences (...). To this end, Member States may, *inter alia*, adopt legislative measures providing for the retention of data for a limited period justified on the grounds laid down in this paragraph.'

The same article indicates that the adoption of such measures will respect what is stated in Directive 95/46/EC and, in addition, Article 29 Working Party will assure that these measures respect the rights, fundamental liberties and legitimate interests of the users in the electronic communications sector.

Consequently, the use of mobile devices with IPv6 requires taking into account certain legal aspects which are, in the majority of the cases, similar to the ones that exist with IPv4.

Thus, for example, someone is using a mobile device with IPv6 that includes, in a single equipment, typical characteristics of a personal computer, a mobile phone, a PDA and a GPS. This device is acquired to a telecommunications supplier that also acts like an ISP and that manages a platform of its own services and other kind of services provided by third parties.

The device supplier would have to obtain the consent of the informed user to be able to process his personal data, generated as a result of the use of the mobile device.

Therefore, the service provider should have considered, at the moment of the acquisition of the device and through a contract, the applicable regulation on data protection, referring to, at a minimum, what type of data is going to be processed, the purpose of that processing, how long it will be carried out, which other parties would have access to the data, what purposes (different from the processing of traffic data) cause the processing, which are the legal obligations for retention of data, how the user will be able to request the temporary cease of the collection/processing of data or how he will be able to exercise his rights. Of course, the user will provide his consent only in relation to what he was previously informed about (collected data and purposes of the processing).

Another situation where there is a processing of location data is when the characteristics to locate the device from the network in which it is connected are combined with a GPS to create the route of a trip or the movements of its user in his vehicle.

In this case, Directive 2002/58/EC establishes that location data can only be processed if the user's consent has been previously obtained, for the informed purposes and during the necessary time for that processing, in order to enable the provision of value added services

(for example, providing information of the places the user is travelling or information regarding vehicle traffic, alternative routes, etc.).

According to the Directive, the service provider must inform the users of the types of data which are going to be processed, the duration of such processing and if those data are going to be transmitted to third parties prior to obtaining their consent. Even in cases where users have given their consent, they should have a simple means to temporarily deny the processing.

In another example, also using the mobile device but incorporated to the user's vehicle, it is possible to question what could happen if the vehicle is stolen. In the first place, competent authorities could access to the traffic data created by the stolen device in order to obtain its physical location. Also, having the prior consent of the informed user, it would be possible to access remotely to the device and, for example, through an incorporated web camera, discover what is happening in the vehicle.

In this example, the telecommunications service provider would have to assume the responsibility of not informing the user of the generated data from the robbery of the mobile device until its recovery and simultaneously provide the authorities with all data generated by the use of the stolen device (services used, costs, duration, recorded images, erasure of recorded data, etc.).

Finally, it is possible to question the implications of connecting a mobile device to a network different from the usual one under the viewpoint of personal data processing. For example, when the device is connected to an airport's free wireless network in order to buy an airplane ticket, the wireless network provider will have to decide with the user, by means of an information and consent clause, all the terms regarding the data to be processed, purpose, duration, etc., including the fact that the IP address based on IPv6 and the data that could be associated to it will be processed only with the purpose of enabling access to the wireless network.

Another example could be when the user has to participate in a videoconference with the airline company in order to solve an incidence. In this case, the IP address would be used, simultaneously, for communication originated by the mobile phone and also to access to the wireless network. In this case, it is important to remember that both processing are separated and provided by different service suppliers (telecommunications operator and the wireless network provider). The most relevant issue in this example is the fact that each provider must agree, in a contractual and technical way, to only associate the data related to its own service to the concrete IP. The suppliers will not make data crossings because of the fact that the user is using two different services simultaneously and using the same IP or two IPs with only one Unique Identifier.

In conclusion, it can be stated that although the characteristics of data processing could be different depending on the concrete services that cause them, the use of mobile devices

with IPv6 generates a series of data processing that have to fulfil the principles established in Directive 95/46/EC and Directive 2002/58/EC, which already have been analysed through Chapter III of this publication.

5.8. IPv6 in Home Automation

One of the areas seeing recent advancements by Home Automation is household appliances. In this respect, Home Automation has come to be defined as *'the simultaneous use of the electricity, electronics and computer science, applied to the technical management of the home'.*

In particular, some of the aims of by these advances are:

- Energetic Saving: Temperature control, lighting, consumption, etc.
- Security: Custody and intrusion alertness, floods, fire, gas leaks, personal safety, etc.
- Communications: Access to Internet, internal communications, computer resources sharing in a home.
- Comfort: Heating programming, automatic watering, etc.

Home Automation uses a multitude of devices that can be distributed around the entire home depending on the needs of the owner. Basically, these devices can be sensors with sufficient capacity to implement a 'home area network'.

With regard to the present study, it is interesting to be aware of the possible implications concerning the use of the protocol IPv6 in household appliances.

For example, in the event that each one of the different devices in a house has its own IP address with a Unique Identifier used to access the Net, the agents who have the possibility of gaining access to the results of the surfing or access undertaken with those IP's, might obtain valuable information such as the profiles of consumption of the house holders, their routines, their preferences, etc.

Similarly, this possibility could be increased under a probable situation where all the devices in the house had the same prefix in their IP address, serving as a constant identifier.

Nevertheless, from a data protection point of view, it is important to highlight that:

- The creation of profiles, without obtaining the data subject's consent, is a problem that has existed with previous versions of the Internet Protocol and, therefore, it is not a problem caused by the use of IPv6.
- It is not easy for one agent or provider to access these IP's or to group all those in a house in order to obtain profiles.
- The creation of profiles is lawful if it is carried out with the fulfillment of the measures contained in the Directive and in the domestic legislation adopted by the Member States regarding data protection.

Personal Data Protection

- One IP address that is considered as personal data by a particular agent or service provider may not always be considered personal data by a different one.

Supposing that an IP address can be considered as personal data and regarding a particular case where, whether a unique prefix for all the elements of the household's Home Automation exists or not, it is possible to identify the IP's user (e.g. by means of public guides), the requirements that are necessary for data processing can be different, depending on the use or service provided by the Home Automation element.

We can imagine the case of a device with its own IP number, which is used for a tele-assistance service for all members of the family, accessible by means of an individualized identification with a biometric device.

In simple terms, there are three parts implicated in providing the service: the supplier of the necessary telecommunication, the supplier of the service (that also provides the device) and the users.

Referring to the telecommunications supplier, the only data that could be associated with the IP based on IPv6 of the Home Automation device, is that data necessary for management, billing and collecting the traffic generated in the use of the device, as well as, in this case, the other data provided by the device's holder that could be obtained and processed.

With respect to this second type of data, the telecommunications supplier must have informed the user as to what kind of data is collected, with what aim, how long will the data be processed, what other entities are going to access the data and how could the user exercise his rights. Next, the supplier will have to obtain the consent of the user on each one of the mentioned issues. The fulfilment of both obligations could be done by means of agreement clauses regulating the use of telecommunications associated to the use of tele-assistance device.

The service and device supplier also must comply with the obligations of information and consent relative to the personal data processed in the use of the tele-assistance service. Nevertheless, this supplier would also have additional requirements to fulfil.

Thus, for a family using tele-assistance services, it is very probable that health data processing will be necessary (for example, blood pressure, body temperature, symptoms communication, medication communication, etc) and, therefore, obtaining an explicit consent would be required. This consent has to be obtained from each one of family members (except from minors who are under the authority of their parents), by means of the tele-assistance agreement, or specific agreements or clauses.

As mentioned, one of more frequent legal matters in relation with Home Automation is the creation of profiles relative to the family as a whole or to each one of its members.

For example, we can think about the legal implications that would be necessary to consider in creation of customized living quarters environments (for example, state machines that determine light intensity, temperature, control of blinds, television schedule, etc.) and its combination with dietary habits associated with the month of the year that corresponds. Furthermore, we can consider that these services are controlled by an external entity which manages the correct environment creation, automate supplying of food and the reading of RFID (Radio-Frequency Identification) labels included in user clothes and in certain foods.

Reflecting on the reference to information and consent, we can focus on the profiles creation. As it was established, the profiles creation is allowed only when it is in accordance with Directive 95/46/EC and, logically, in accordance with data protection legal framework applicable in each Member State.

However, the user will always have the rights, recognized by the Directive, to access, rectify, cancel or object his profile data obtained until a certain date (data of the person associated to his IP based on the IPv6 and his household's Home Automation element). This could be achieved in order to avoid modifications to the living quarter's temperature (caused by reading the RFID clothes labels), or to limit the automatic re-supply of certain foods such as particular dietary foods included in the medical treatment, harvest foods, etc, or even to avoid the television programming blocking those contents prohibited for minors.

Another important aspect can be considered related to the supplier managing the customized environment and the automatic food re-supply based on the month. This supplier is usually going to use other entities' services, for example, to generate and deliver a virtual delivery based on reading RFID labels or bar codes, digital photographs of refrigerator, etc.

In the event these third parties have access to the user data associated with the IP of the refrigerator in order to render services, managing the re-supply for example, they must regulate such circumstance in agreement with the rules regarding the relationship between the principal supplier and this subcontracted third party supplier. The agreement must indicate, at a minimum, what IP data, based on the IPv6 user, are going to be obtained because of the service, how the principal supplier is going to transmit the orders to the subcontracted supplier, and what is going to happen with the data once the service is rendered (IP and other associated personal data).

In conclusion, the use of Home Automation by means of devices based on IPv6 continues to receive similar legal problems and legal solutions that are occurring with IPv4. Nevertheless, the development of the new protocol could be an opportune moment to identify and regulate the aspects relative to the personal data processing derived from use of such devices based on IPv6.

5.9. Security Measures to be adopted in the Processing of IP Addresses

The various Directives in force on Data Protection oblige the controllers (persons in charge of the personal data processing) to adopt technical and organizational measures that, besides guaranteeing the confidentiality of the information and its correct processing, bring about security.

In this respect, none of those Directives set out an approximate set of safety measures to be adopted by the Member States, which means that, sometimes, these States have their own legal regulations but with different contents.

With regard to the implementation of safety measures, it is important to highlight that the new Protocol IPv6 includes a security protocol called IPSec through which it guarantees, among other matters, the following:

- Authentication of the origin of the information and, therefore, the possibility of not receiving communications sent by users which are identified by a certain IP.
- Integrity of the information transmitted.
- Confidentiality of the information.

In conclusion, it is important to say that the matters raised by this security protocol IPSec will be analyzed in next Chapter of this publication, because of the implications that its adoption could have in the struggle against piracy and in the defence of intellectual property rights, copyrights, etc.

6. The use of RFC3041

6.1. Brief Explanation of how it operates

As stated above, in respect of the unique number (IP address), IPv6 pioneered a labor saving way for 'interface identifiers' to be formed automatically in devices, as one of the various methods of setting up addresses. The privacy concern related to the fact that both this and the interface identifiers in 'always-on' environments result in permanent numbers as part of the addresses and allow the tracking of individuals.

Market researchers use techniques (data-mining) that can track Internet usage and, if addresses don't change, match them to individuals. This is of particular concern with the expected proliferation of next-generation Internet-connected devices (e.g., PDAs, cell phones, etc.) that could be associated with individual users. With the growing use of 'always-on' links (DSL, cable modems), users are increasingly subject to data mining that tracks their unchanging Internet address.

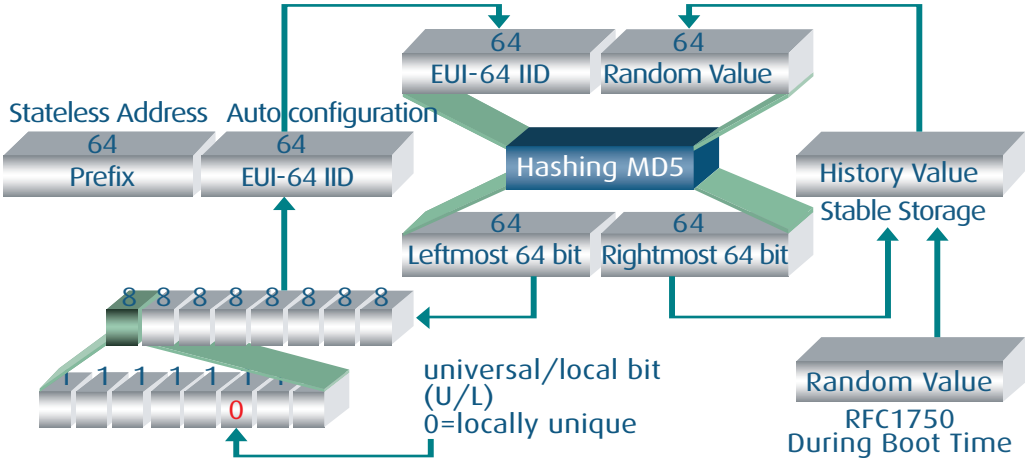
Thomas Narten and Richard Draves of Microsoft Research published a procedure to deal with this issue and ensure privacy of IPv6 users - RFC3041 titled 'Privacy Extensions for Stateless Address Autoconfiguration in IPv6' published in January 2001 by the IETF. The procedure works

on the basis of an algorithm developed jointly by Narten and Draves, which generates randomized interface identifiers numbers and temporary addressees during a user session for outgoing communications. Randomly generated numbers would replace the unique interface identifier and RFC3041 standardized how and when that would be done. The aim of this was to eliminate the concerns privacy advocates had with IPv6 by generating a random identifier(s) for the same node for outgoing communications making it difficult to determine the connection between a node and an individual.

The summary at the beginning of the document states:

'Nodes use IPv6 stateless address autoconfiguration to generate addresses without the necessity of a Dynamic Host Configuration Protocol (DHCP) server. Addresses are formed by combining network prefixes with an interface identifier. On interfaces that contain embedded IEEE Identifiers, the interface identifier is typically derived from it. On other interface types, the interface identifier is generated through other means, for example, via random number generation. This document describes an extension to IPv6 stateless address autoconfiguration for interfaces whose interface identifier is derived from an IEEE identifier. Use of the extension causes nodes to generate global-scope addresses from interface identifiers that change over time, even in cases where the interface contains an embedded IEEE identifier. Changing the interface identifier (and the global-scope addresses generated from it) over time makes it more difficult for eavesdroppers and other information collectors to identify when different addresses used in different transactions actually correspond to the same node'.

The Stateless Address Autoconfiguration is a mechanism to create a 128-bit IPv6 address. The left hand 64 bit is the 'prefix' and the rightmost 64-bit is the unique identifier or EUI-64 IID.



How Interface ID is Created using RFC3041?

As seen from the diagram above, a random number would replace the EU1-64IID. The mechanism would attach a 64 bit random value to the EUI-64 IID for history purposes and a hashing algorithm would take place. This is a one-way algorithm that cannot reconstruct the original number. This algorithm would create a new random 128-bit number. The leftmost 64-bit forms part of the Stateless Address Autoconfiguration (which now has no link to the appliance as it is a randomly generated number not based on the unique identifier) to create an IPv6 address and right identifier remains as stable storage to prevent duplication.

This address would be used for outgoing communications. The terminal equipment uses two types of addresses: N address is generated based on the unique MAC address, and is used for entering communications (e.g. the terminal is always reachable using that permanent address), and another RFC3041 address generated on a random basis, to be used at the initiative of the terminal for outgoing connections. Thus, when the terminal (and the user behind) is responsible for the connection, it could not be identified through its MAC address.

At first, it could be said that if RFC3041 is widely implemented, it could provide a solution to the privacy issues presented above.

6.2. What Force does it have?

RFC3041 is a 'Standards track' RFC and it is currently in the category of a 'proposed standard' (PS), which is the third of the three levels of maturity set out in above.

Given that it is only a proposed standard, the force of the document may be called into question.

However given the way that the Internet has developed, many things being used in daily Internet live (PPP, POP3, IPv6, FTP and TCP extensions, etc.) are still in 'PS' category due to the fact that the IETF process is slow. Many of these things have the force of being a standard through widespread acceptance and implementation, which provide them with the 'de facto' standard status. RFC3041 has been implemented in Microsoft Windows XP/2003 and Linux operating systems and the force of this speaks for itself.

6.3. Implications of its Adoption from the Data Protection Point of View

If the adoption of this standard could prevent certain agents from discovering the Unique Identifier of a certain IP address, at first, it could be stated that this address could not be associated with a certain device by the agent, and, therefore, with a concrete user. Likewise, it would not be possible for him to trace its movements along the Net.

As a consequence, for this agent, this IP address could not have the consideration of personal data and, therefore, they would not have to comply with the obligations imposed by data

protection regulation since, in these circumstances, the above mentioned information would be considered as anonymous information.

These assertions will be valid, in case the above mentioned agent does not have alternative means to be able to identify the device to which the above mentioned IP address is linked.

On the other hand, in spite of the use of this measure, by necessity, other agents will have to still know the real IP address that contains the Unique Identifier, for example, to provide their services. Therefore, they will continue to be obliged by the obligations imposed by the data protection regulation.

Though this technical measure would be applicable to the majority of the situations, it has been determined that RFC3041 is not applicable to mobile IP's. In these cases, the different agents would continue to be obliged because of this type of IP's.

6.4. The Use of RFC3041 by the Manufacturers of Hardware and Software

Following the recommendations made by Article of 29 Working Party, the manufacturers will have to adopt the necessary technical measures, required at all times, which guarantee the privacy of the users.

Likewise, Directive 2002/58/EC, in its Preliminary Consideration Number 46 establishes that *'it may therefore be necessary to adopt measures requiring manufacturers of certain types of equipments used for electronic communications services to construct their product in such a way as to incorporate safeguards to ensure that the personal data and privacy of the user and subscriber are protected'.*

In this respect, it is recommended that manufacturers (software and hardware manufacturers), enable users to use this type of device or, on the other hand, of accessing the Net avoiding them. In this way, they should inform the users, by way of standardized informative clauses, about the possibilities afforded by these mechanisms and the consequences of their use.

In this sense, in spite of the possible technical difficulties that could exist for their implementation, there would be several different possibilities for these manufacturers in adopting them:

- OPT OUT: According to this system all manufacturers must incorporate in the elements which form part of the hardware or software elements that they produce, devices of this nature based on the RFC3041 or on any other standard of this nature. If the user does not want to use this type of tool, he should request its 'deactivation' by his manufacturer or corresponding provider.

- OPT IN: On the other hand, this new method would suppose that manufacturers would not include, in a general way, this type of tool in hardware or software elements that they generate but, on the other hand, they would remain obliged to give the option to the users to acquire them, informing them about the way to use them and about the consequences of their use.
- Intermediate System: Through this system, the manufacturers will be able to give the possibility to the users of their products to activate or deactivate this technical solution, depending on whether they wish to access anonymously or not.

This third option appears, at first, as the most suitable one since, in certain situations, it will be necessary for the user to access with a recognizable IP.

6.5. Other Relevant Considerations

The implementation of IP addresses based on Unique Identifiers has given rise to certain opinions regarding the fact that, in addition to the implications of its implementation on the users´ right to privacy, the use of this kind of IP´s could be contradictory in relation to one of the principal characteristics of Internet: i.e. its anonymous character.

For this reason, the development of technical measures based on the RFC3041 probably will have a good reception in certain sectors. Nevertheless, some doubts have appeared regarding its utilization, for example, the fact that these measures may cause the obstruction of judicial or police investigations relating to the commission of criminal or unlawful activities.

Therefore, it would be appropriate to determine which agents or bodies on the Internet, for example, access providers, would continue to have the possibility of identifying a certain IP address from its Unique Identifier, in spite of the use that could be made by a user of the technical measures mentioned above, in protection of his anonymity. This point is especially relevant because this possibility would turn this type of agent or body into the main means of collaborating with the relevant authorities in the pursuit of criminal and unlawful activities committed while using Internet.

7. What steps have been taken to achieve a european consensus on IPv6 and privacy?

7.1. The Role of the European IPv6 Task Force

The European Commission set up an IPv6 Task Force ('EC IPv6 TF') in 2001 to help with the widespread deployment of IPv6 in Europe and one of its role's was to answer queries or criticisms raised about IPv6. Some of the EC IPv6 TF members are also involved in the Euro6IX project and both parties have a mandate to see the privacy issues dealt with effectively.

Personal Data Protection

The EC IPv6 TF was concerned that the Article 29 Working Party Opinion (WP58) potentially resulted in an unbalanced view of the benefits of IPv6 and therefore organized a meeting with the Internet Group of the Article 29 Working Party ('Article 29 WP') to try and discuss this issue in more detail and explain the privacy enhancing features of IPv6. Several partners of Euro6IX and the IPv6 Task Force formed part of the group that attended a meeting in Brussels on 25th February 2003 on this specific issue.

The EC IPv6 TF published a position paper prior to the meeting, which made the following points:

- The EC IPv6 TF recognizes that the use of unique identifiers in any kind of technology or communication media (e.g. Ethernet, WLAN, GSM, ID cards, IPv4 and IPv6) represents a potential threat to privacy.
- But the EC IPv6 TF also notes that the use of stable identifiers is an important practical requirement in any communication system.
- All communications are subject to privacy issues and IPv6 is no exception.
- IPv6 has provided a mechanism (RFC3041) that goes a long way to solving the problem, potentially providing a higher degree of protection to the users than is possible in IPv4.
- In addition IP security (IPSec) mechanisms are available in full IPv6 implementations (RFC2460). Although their use is not mandatory, this offers an improvement over IPv4, where IPSec support is not present by default.

'The following key considerations must be taken into account when reviewing the privacy implications with IP based communications, both for existing IPv4 and the emerging IPv6.

1. IPv4 has privacy issues with static IP addresses being used as identifiers. These can be tracked just as other devices and items used by a person can be.
2. IPv6 by default where stateless autoconfiguration is used will construct IPv6 addresses that allow the correlation of activity where the same device is connected to different networks because a constant identifier (based on hardware in devices) is embedded in the IPv6 address.
3. RFC3041 fixes the problems of correlation by allowing an IPv6 device to generate a random identifier to embed in the address.
4. Many Internet systems use IP addresses as a (weak) authentication mechanism. Use of privacy extensions prevent such authentication being used. However, IPv6 includes IPSec by default, allowing stronger authentication methods to be used.

Personal Data Protection

5. IPv6's Privacy Extensions enable a static host (e.g. workstation in the office) to use different IPv6 source addresses through time (e.g. a different IPv6 source address daily), allowing greater privacy for such non-mobile devices and users.
6. It is normal practice for IPv6 devices to have multiple addresses, where IPv4 devices usually have one address. It is thus possible for future IPv6 applications to use multiple (dynamic) IPv6 addresses, e.g. to reduce traceability in peer-to-peer applications.
7. Further research may introduce new classes of IPv6 addresses, for example cryptographically generated addresses. This is only possible with IPv6.
8. The EC IPv6 TF strongly recommends that vendors implement RFC3041 by default in all systems. The TF notes that some vendors have already done so.
9. There should be easy user-controllable mechanisms for RFC3041 to be enabled or disabled, per device/interface or per application. This could also be automatic depending on the initiated traffic (in bound or outbound), pre-configured by default or customized. These may require further work or research. Again, such enhancements are only possible with IPv6'.

The EC IPv6 TF stated that 'the privacy issue is one (important) piece of the larger chess-game of security, transmission, e-business, open government, law enforcement and even good governance. So in any intergovernmental recommendations on this area it would be useful to see a more interdisciplinary approach emerging in the future.'

'The EC IPv6 TF believes that the new built-in properties in IPv6 provide a set of necessary and unique tools to empower a user's privacy in ways that are not possible in IPv4. The combination of the availability of IPSec support in full IPv6 implementations combined with these new properties makes IPv6 a potentially powerful tool to improve the possibilities for user privacy.

The EC IPv6 TF strongly recommends the implementation of RFC3041 by all IPv6 vendors. However it is clear that in any communication medium a balance needs to be struck between usability and privacy. For example, further work would be desirable on allowing user-controllable enabling of the IPv6 privacy extensions on a per-application basis'.

In view of the above the EC IPv6 TF asked the Article 29 Working Party to reconsider its statement given the fact that IPv6 had significant improvement in relation to privacy in comparison to IPv4 and stated that a statement by them would be an important signal to the IPv6 community who had viewed the paper with some concern.

7.2. Meeting with Article 29 Working Party in Brussels on 25th February 2003

As stated above, after publishing this paper, the EC IPv6 TF went to Brussels to meet with the Internet Group of the Article 29 Working Party.

The IPv6TF presented its position (http://www.ec.ipv6tf.org/in/i-documentos.php) and gave a short overview of RFC3041. The EC IPv6 TF wanted to make clear that the following key considerations should be borne in mind when looking at the privacy implications of IP based communications both in IPv4 and IPv6:

IPv4 has privacy issues with static IP addresses being used as identifiers. These can be tracked just as other devices and items used by a person can be.

IPv6 by default where stateless autoconfiguration is used will construct IPv6 addresses that allow the correlation of activity where the same device is connected to different networks, because a constant identifier (based on hardware in the device) is embedded in the IPv6 address.

RFC3041 fixes the problems of correlation by allowing an IPv6 device to generate a random identifier to be embedded in the address.

It was generally agreed that the meeting of the EC IPv6 TF and the Article 29 Working Party had been a good step, that it was important to proceed together. The Article 29 Working Party was in principle willing to enter in a dialogue with the EC IPv6 TF as stated in the Opinion paper. The Article 29 Working Party offered to do some work in the Euro6IX project. There are two deliverables later this year and it was agreed that members of the Article 29 Working Party would have the opportunity of reviewing the document to reach a consensus with the EC IPv6 TF.

8. The problem of the extraterritoriality

8.1. Some Problematic Cases

In many cases, it may be difficult to determine what legislation, in this case, on data protection, would be applicable to certain data processing, principally, when these are carried out in the Internet.

One example of this problem could be the following: a web page located in a certain Member State (for example, France) through which, information is obtained by its Internet users from any country of the world and whose holder and, therefore, person in charge or controller of such files, is an entity whose nationality belongs to one of the Members States, for example, Spain.

Personal Data Protection

The mere storage of information is considered as personal data processing. Therefore, in the described situation, there would be two agents who are processing personal data, so two different sets of regulations exist which might be applied to this processing.

Whilst this situation would give rise to problems regarding the determination of the applicable regulation, in any case, the physical and legal safety of the obtained information would not be in danger, because both States (France and Spain) have their own data protection legislation based on the Directive 95/46/EC.

Now let's think about a new situation that could give rise to major complications. The web page is located or hosted in France but the holder of the web page and person in charge of such information belongs to a State that has not adopted any regulation on data protection. How could this information be protected?

8.2. General Aspects to be considered

It could be noted that this problem happens not only because of the implementation of IPv6. On the contrary, it is an intrinsic problem for the Internet.

Although it is clearly tremendously difficult to adopt, around the world, a single set of legislation which tries to solve this problem, at least from the perspective of the European Union, it would be necessary to continue with the current plan of action, characterized by the desire to create and form a common, clear, strict but at the same time flexible set of regulations, that enables the resolution the major problems that arise from the processing of personal data, as well as to increase the agreements with different foreign States not included in the EU concerning these matters, focused on the previous education and awareness on data protection.

Thus, Member States and those with recognized levels on data protection, will have to, gradually, adapt their regulations to the legal initiatives adopted, as an answer to the new problems which have arisen in relation to personal data processing.

8.3. The Power of Self-Regulation

Nowadays one of the principal methods being adopted on the Internet (among other sectors of activity) trying to lessen the effect of the lack of specific regulation on certain topics, is the self-regulation or the adhesion to codes of conduct produced by different sectors, through which have been generated a series of procedures or 'good practices' that govern the activities of the members of this sector adhering to the code until a specific regulation is provided.

According to this idea, the Preliminary Consideration Number 61 of the Directive 95/46/EC establishes that*: 'Whereas Member States and the Commission, in their respective spheres of competence, must encourage the trade associations and other representative organizations concern to draw up codes of conduct so as to facilitate the application of this Directive, taking account of the specific characteristics of the processing carried out in certain sectors, and respecting the national provisions adopted for its implementation'.*

As it could be expected, although this option appears useful, there is a problem and it is that the abovementioned codes do not bind those agents who do not adhere voluntarily to them.

Some of the matters that should be contemplated in the Codes alluded to and whose adoption by the different agents would be suitable, would be, among others, the following:

- Prohibition of processing personal data (including IP addresses) for different purposes from those which are necessary to provide the services contracted by the users (i.e. provision of access to the Net; providing of some concrete services, etc.).
- Obtaining the users consent by using some standard clauses set out in the above mentioned Codes. This consent must be obtained by the agents, which are going to process personal data with different purposes from those which the user was previously informed of at the moment of the introduction to the services to be contracted (i.e. profiling of the user by tracing his movement on the Net).
- Obtaining the users consent to enable the agents to forward their personal information to third entities (i.e. to obtain their consent to be able to transmit their IP address to an entity in charge of the management of public guides or directories or to send the above mentioned information to companies dedicated to the production of advanced users profiles, etc).
- The setting out of a series of security measures that should be applied by virtue of the different types of information that these agents could process in their daily activity, giving a guarantee in relation to the confidentiality and integrity of this information.

In this respect, the Directive 95/46/EC already establishes this need in its Preliminary Consideration Number 46 when sets out: *'Whereas the protection of the rights and freedoms of data subjects with regard to the processing of personal data requires that appropriate technical and organizational measures be taken, both at the time of the design of the processing system and at the time of the processing itself, particularly in order to maintain security and thereby to prevent any unauthorized processing; whereas it is incumbent*

on the Member States to ensure that controllers comply with these measures; whereas these measures must ensure an appropriate level of security, taking into account the state of the art and the costs of their implementation in relation to the risks inherent in the processing and the nature of the data to be protected'.

Finally, it is necessary to emphasize that it would be suitable that these types of codes are adopted by the providers of technical solutions for hardware and software elements, in order to assure the confidentiality of the personal data and the privacy of the users. Thus, the abovementioned providers would remain informed about certain practices that they should develop with the purpose of protecting the user's rights to privacy and data protection.

For example, one of the main points to include in such codes, would be the obligation to inform the users of the existence of these technical measures and of the consequences of their adoption or of the lack of their adoption in relation to the protection of the above mentioned rights.

9. Conclusions

This section sets out the principal conclusions of this study regarding the implications on data protection of the implementation and use of the new Protocol IPv6:

1. The standardization of the implications on data protection resulting from the implementation and use of IPv6 must be a top priority, so that the different entities, authorities and citizens, increasingly conscious of their rights and obligations on this matter, can have total confidence in the safety of this Protocol in connection the processing of personal data.

2. Data protection refers to the legal protection of individuals concerning the automatic processing of their own personal data. In this respect, personal data is considered as any information relating to an identified or identifiable natural person. Therefore, an IP address would be personal data if it is possible to associate it to a certain natural person, direct or indirectly.

3. Using IPv6, the IP addresses based on a Unique Identifier allow the association of these IP's with the nodes or devices that are using them. Then, if it is possible that an agent associates it with its holder, by any means, for example, through the contract that a provider has entered into with this holder or by other means like the use of public guides, these IP's will be deemed to be personal data and their processing will remain governed by this regulation.

On the contrary, if the agent does not have the possibility of association open to him, this IP address would not be considered as personal data.

4. Directive 95/46/EC is the fundamental regulatory framework on data protection, through which the basic principles and obligations applicable to all personal data processing have been established. Its provisions may be considered to be directly applicable to the processing derived from the use of the Protocol IPv6 and, therefore, since the consequences of the processing of this type of data do not differ or contradict the principles, obligations and rights stipulated in this Directive, it should be concluded that, at first, it would not be necessary to modify the Directive.

5. Directive 2002/58/EC is the community regulation that tries to standardize the specific requirements on data protection regarding the new services of electronic communications. Some of its main considerations are the following:

   a. Consideration of the information related to the IP addresses as traffic data. Any processing based on different purposes other than the ones which are necessary for the conducting of communications, the billing of the service or as a proof of the performance of a commercial transaction, as a general rule, the consent of the holder (data subject) will be needed to enable this processing.

   b. The Directive allows the users who originate a communication, to request the restriction of the identification of the line of origin as well as to the user who receives them, to reject those which come from non identified lines. Analogically, this practice might be applicable to IPv6, which is being done by using technical solutions based on the RFC3041.

   c. An IP address can be considered as location data which enables the finding out of the geographical location of a concrete terminal or node. In this case, the possibility similarly exists of identifying the location of the user of this terminal.

   d. Public guides or directories are one of the means that would allow the association of a certain IP with a certain user and, therefore, that would promote the consideration of IP addresses as personal data. Nevertheless, it is important to highlight that the regulation offered by the Directive is not totally adjusted to the nature of the IP guides which might be created, since its regulation is orientated to telephone directories.

Personal Data Protection

6. The implementation of IPv6 means that some processing of information that, previously, was not bound by the data protection regulation because the processing was carried out over anonymous information, now, begins to be covered by this regulation. Specifically, this processing is carried out in relation to the information an IP address itself and the one produced by the information associated with those IP addresses.

7. One of the principal problems detected with regard to the implementation of IPv6 is the possibility of tracing the activities undertaken by the user connected to the Net, for example, while he is surfing, and associating the results of the above mentioned tracing with a concrete node or device and, potentially, with its holder or person who has carried them out.

   These activities, at first, would not always be considered as unlawful. On the other hand, these kinds of processing could be lawful if they are carried out in compliance of what it is established on the current regulation.

   In this sense, the Common Position regarding online profiles on the Internet, adopted at the 27th meeting of the Working Group on 4/5 May, 2000 in Crete, establishes for the Internet service providers the obligation to inform the users about this type of processing and the obligation of obtaining their consent.

8. The generation of profiles, without the previous collection of the data subject's consent, are a problem that has existed with the previous version of the IP protocol and, therefore, it could be stated that it is not a problem initiated by the use of IPv6. With regard to this, the obtaining of a profile is lawful if it is carried out in compliance to the provisions contained in Directive 95/46/EC and in the legislation adopted by every Member State.

9. If the adoption of the RFC3041 prevents certain agents from knowing the Unique Identifier of a certain IP address and preventing him from linking to the device and its holder, the information of an IP address, to the above mentioned agent would not be considered as personal data and, therefore, this agent would not remain obliged to fulfill the obligations imposed by the data protection regulation.

   It is recommended that an obligation is established for software and hardware manufacturers to give users the possibility of using devices based on this standard or, on the other hand, of accessing the Net through other means. In any case, these

manufactures should inform the users, by means of a standardized informative clause, of the possibilities afforded by these mechanisms and the consequences of their utilization.

10. The extraterritorial character of the Internet raises, in many situations, problems relating to the determination as to what legislation should govern certain processing of personal information.

11. One of the principal means that are being adopted to relieve the lack of specific regulation on the Internet is self-regulation or the adhesion to codes of conduct produced by different sectors of activities. In this respect, the Directive 95/46/EC promotes the creation of these types of codes by the Members State, regarding the protection of personal data.

In general, it could be stated that IPv6, in regards of this document, is not worst than IPv4, on the contrary, provides means for increasing the privacy of the users, which can't be done using IPv4.

Nevertheless, is also important to track and consider existing and future works regarding the IPv6 implementation (i.e., draft-dupont-ipv6-rfc3041harmful-04.txt), that could imply future legislation amendments.

Intellectual Property Rights and Copyrights

1. Introduction

The technological advances produced during the last decades have given rise to means that facilitate the transmission of information in electronic format, in enormous volumes, through telecommunication networks.

One of the principle legislative facets to analyze is that relating to the protection of contents transmitted by telematic networks that are found protected by the Intellectual Property legislation.

Certainly, not all the information transmitted by electronic means, i.e. by Internet, is susceptible to being protected by Intellectual Property, but it is important to emphasize that the volume of protected contents is considerably significant. Furthermore, the previously mentioned increase in volume of information transmitted by new and improved technologies, i.e. IPv6, assumes the corresponding increase in susceptible contents to be protected by the Intellectual Property legislation.

Regarding this context, the principal aim of the present Chapter is to outline the relations that possibly commence between the development of IPv6 and the Intellectual Property legislation, a concrete example, being the characteristics of the new Protocol that can be utilized to manage or improve the protection of Intellectual Property Rights (IPR).

It is widely known that IPv6 does not have as its own objective for the protection of these rights nor the creation of formulas for such a task. As such, the analysis put forth of the Protocol, its applicable legislation, the current problems regarding the transmission of information by Internet, etc. must be conducted from the perspective of determining what characteristics of IPv6 could extend their use towards the protection of the IPR and, as a result, towards the improvement of managing contents of an electronic nature, where IPv6 is going to have a fundamental role.

It is necessary to highlight that the conclusions extracted from this Chapter, regarding the protection of the mentioned rights, will be applicable only to that data transmitted over communication networks, making use of the new Protocol, which would be susceptible to protection by the Intellectual Property legislation.

To these ends, this Chapter achieves a closer relationship to the concept of Intellectual Property and adopts the principal characteristics of the susceptible objects of IPR (patents, trademarks, industrial designs and copyright), always focusing the attention on the most interesting characteristics in relation to the aims of this book.

Once these concepts are established, this Chapter will continue with a section dedicated to the principal references to the Intellectual Property legislation in the European Union in order to articulate the most significant aspects between IPv6 and Intellectual Property found within the community legal framework.

Intellectual Property Rights and Copyrights

Thereafter, the main challenges and problems confronting Intellectual Property within an electronic scope will be analyzed, followed by the fundamental sources of influence that the new Protocol IPv6 may experience within the field of IPR, thus intending to show those elements of the Protocol that could be utilized for the protection of the already mentioned rights.

As a result of this, this Chapter establishes that one of the principal characteristic of IPv6 regarding the protection of the IPR could be seen as the Security IPSec Protocol, currently used with version 4 of the Protocol (IPv4). With the new Protocol, new characteristics will be reinforced and will become intrinsic elements, thus making it an aim to establish exactly how these security characteristics related to the transmission of information can improve the protection and management of contents susceptible to IPR.

2. Intellectual Property

2.1. Concept

The study of the legal consequences due to circulating contents protected by IPR through telematic networks, public or private, makes it not only necessary to manage the features that can contribute to the transmission and use of the new Protocol IPv6, but also, it is interesting from the following two different perspectives:

- The new ways of violating the IPR that have generated as a consequence of the technical possibilities of suppressing technological barriers to protecting rights as well as the possibilities of transmitting information between the participants in electronic communication.
- The necessity of a flexible legislation that guarantees assuring protection of the IPR, intending to create a regulatory framework that not only focuses its attention on the electronic means of exploitation that currently exist, but also would be capable of assuming the regulation of probable future exploitation as a consequence of the incessant growth of new technologies.

However, before continuing, the concept 'Intellectual Property' must be clarified, seeing as it is a broad legal concept containing certain elements or parts of interest to the present Chapter.

Intellectual Property relates 'to creations of the mind: inventions, literary and artistic works, symbols, music, images, audiovisual works and drawings and models used in commerce'(2).

The categories dividing Intellectual Property in the community space, independently to the fact that the legislations of certain member countries (i.e. Spain) are structured in a different way, follows the outline of the World Intellectual Property Organization (WIPO), which are:

Intellectual Property Rights and Copyrights

- 'Industrial Property, which includes patents, trademarks, industrial designs and geographic indications of source.
- Copyright, which includes literary works such as novels, poems, plays, movies, musicals, and artistic works such as drawings, paintings, photographs, sculptures and architectural designs'(3).

In addition, the related rights are 'those of performing artists in their performances, producers of phonograms in their recordings, and those of broadcasters in their radio and television programs'(4).

Before beginning the section of this Chapter that covers the principal characteristics of each of the protected objects under Intellectual Property, always highlighting the most relevant elements in regard to IPv6, it should be understood that not all the information, data, files, etc. that circulate through telematic networks, for example, Internet, are susceptible to IPR. Because of this, the considerations made in relation to the influence of IPv6 on the protection of IPR refer only to those contents transmitted by telematic networks that are susceptible to the application of such rights, for example, music, movies, photographs, literary work, software, etc.

2.2. Description of the Protected Objects

The present subsection establishes, in brief, the descriptive items of each category for the protected elements, focusing on those that could result most significant regarding the present Chapter, those that could be useful in configuring the role of IPv6 in protecting the IPR within the electronic scope.

2.2.1. Patents

A patent is an exclusive right granted to an invention, which is considered either a product or a process offering a new way of achieving a product or rendering a service or developing new ways of achieving or rendering services currently functioning.

A patent provides proportioned protection to the inventor, which is provided during a limited period of time, normally 20 years.

In addition, the details of the invention should be published. This means that, in spite of the concession to the inventor's patent, the technological development diffuses after the moment in which the patent details have been made public and can be exploited by third parties after the patent having expired.

It is important to reiterate that only certain types of inventions can be patented. Such examples

(2), (3) and (4) http://www.wipo.org

would be inventions (in other words, products or processes) qualifying as novelties that are not obvious to a person familiar with the technology or related art field of the new patent. It is not possible to patent a known invention.

From a legal perspective, the protection of a patent means that the invention cannot be fabricated, utilized, distributed, commercially sold, etc. without the consent of the patent holder. In other words, the inventor is the person who has the right to decide who can and cannot use the patented invention during the period of time the invention is protected.

However, the patent holder can articulate ways of usage by third parties, through licenses, whose conditions establish a common agreement between the patent holder and the licensee. Furthermore, the patent holder can transmit his rights to the invention to a third party, for example, through purchase. In this case, the third party assumes the conditions as a holder of the patent.

Finally, it is important to mention that once the patent expires, so does the protection, therefore extending the invention to the public. Thus, the holder relinquishes his exclusive rights to the invention, which becomes available for commercial exploitation by third parties.

2.2.2. Trademarks

A trademark is a distinguishing sign susceptible of graphical representation that indicates that certain goods have been produced or certain services have been rendered by a person or determined company.

Trademarks can consist of one word or a combination of words, letters and numbers. They can also consist of drawings, symbols, three-dimensional characters, auditory signals, colors or other elements that can be used as distinguishing characteristics.

In this way, a trademark offers protection to the holder, guaranteeing exclusive rights to use the trademark in order to identify its goods or services or to authorize a third party to use the trademark in exchange for payment.

One of the main objectives to the system of using trademarks is to hinder the efforts of unfair competitors, for example, counterfeiting, who use similar distinguishing signs in order to recognize products or services distinct from those protected by a trademark which, in many cases, are of lesser qualify. In the electronic field, where IPv6 plays such an important role, the system of using trademarks serves, among other ends, to hinder and track the illegitimate use of distinguishing signs or trademarks by unauthorized third parties thus committing an infraction of the IPR (i.e. domain names, the use of logos in websites without authorization, the sale of falsified products on the Internet, etc.).

In addition to the trademarks that identify the commercial origin of goods and services, there exist other categories of trademarks. For example, collective trademarks are property

of an association whose members use them in order to identify what to account for, referring to a determined level of quality and other requirements established by the association. Another type are certification trademarks granted to products that satisfy determined norms, but do not restrict solely to organization members. These trademarks can be granted to any member that can certify that the products in question satisfy certain established standards (i.e. ISO 9001).

2.2.3. Industrial Designs

An industrial design can be defined as an ornamental or aesthetic aspect to an article. The industrial design may consist of three-dimensional characters, such as the form or surface of an article, or two-dimensional characters, such as designs, lines and colors.

An industrial design should hold primarily an aesthetic character rather than a functional one, as the legislation does not protect any of the technical characters of articles.

The system of protecting industrial designs is proportioning to the holder (the person or entity that has registered an industrial design), the exclusive right against the unauthorized copying or imitation of the industrial design by a third party.

2.2.4. Copyright

Copyright is a legal term referring to those rights granted to the creators of artistic and literary works.

The types of works protected by copyright are the following: literary works such as novels, poems, plays, reference documents, newspapers, computer programs, databases, movies, musical compositions, choreographies, artistic works such as paintings, drawings, photographs and sculptures, architectural works, publicity, maps and technical drawings.

The important evolution of telematic communication and Information Society has started a plan for new ways to exploit contents protected by copyright, but also has entailed new and serious problems derived from the ease with which one can violate copyrights within the electronic field.

As already mentioned, the technological evolution of mediums for transmitting information in the electronic field permits the sending and receiving of large quantities of information. In many cases, the data or information transmitted includes contents susceptible to IPR. Furthermore, the development of Protocols like IPv6 increases the possibilities of facilitating transmission. It is for this reason that the development of the Protocol should outline which characteristics can be used for establishing, reinforcing or improving the system of protection of IPR. Likewise, it should seek a suitable balance between the improvement and the optimization of the transmission of contents with respect to the IPR.

Intellectual Property Rights and Copyrights

Returning to the determined characteristics of copyright, it must be recognized that the original creators of the protected works, as well as their inheritors, enjoy certain basic rights. Among these, they hold the exclusive right to use the work or authorize its use by a third party for commonly agreed upon work. Thus, the creator of a work can prohibit or authorize the following:

- Reproduction of the work in various forms.
- Its public performance.
- Recordings.
- Broadcasting.
- Translation or adaptation of the work into other languages.

In further detail, copyright is based, principally, in the exclusive exercise of patrimonial rights or the exploitation in any form of the work. The principal patrimonial rights or those of exploitation are the following:

- Right of reproduction, situating the work in a mean that permits its communication and the obtaining of copies in its entirety or in part.
- Right of distribution, referring to the public availability of the original work or its copies by means of selling, renting, lending or any other legitimate act.
- Right of public communication, under which a group of people may have access to the work without previous distribution of samples of such communications.
- Right of transformation, understood as the translation of the work, its adaptation or other means of modifying the work resulting in a different piece.

As it is easily confirmed, each and every one of these rights appears very usually in the field of electronic communications and, as a prominent example, Internet. In addition, the transmission of contents susceptible to these rights are going to be increasingly more important and of more volume due to the advances of the technological developments like IPv6. The transmission of video and audio in real time, the possibilities of file exchange, Internet video on demand, etc. are examples that show the necessity to look for which elements, from the technical aspect, for example IPv6, are opportune for the protection of the rights, i.e. considering the utility that addressing methods (multicast, unicast and anycast) could provide the Protocol.

On the other hand, the protection of copyright includes moral rights equivalent to the right to claim for the authorship of a work and the right to oppose modifications that could be attacking the creator's reputation.

The basis to copyright protection is that only expressions are protected but not ideas, procedures or methods of operation or mathematic concepts.

Intellectual Property Rights and Copyrights

Considering works protected by copyright, related rights have been developed. These are regarded as similar rights, despite being often more limiting and lasting for shorter periods of duration than copyright. These related rights would be granted to the following:

- Interpreting or performing artists with respect to their performances.
- Recording producers respect to their records.
- Broadcasting organizations in their radio and television programs.

In addition, in the field of copyright it is necessary to make reference to the concept of Collective Management of copyright and related rights. This comes from the evident improbability that many of the authors bring to a close their individual management of the patrimonial rights for the works they possess. For this reason the concept of Collective Management has surfaced as an exercise of copyright and related rights by means of organizations that act in representation of the right holders, in defense of their interests.

In general, the organizations of Collective Management exercise the following rights:

- The right of public performance.
- The right of broadcasting.
- The mechanical reproduction rights in musical works.
- The performing rights in dramatic works.
- The right of reprographic reproduction of literary and musical works.
- Related rights.

Finally, it must be highlighted that copyright and related rights are essential for the human creativity by offering the authors incentives in the form of recognition and corresponding economic compensation. This system of rights guarantees the creators the circulation of their works without fear of unauthorized copying or pirating acts. At the same time, this contributes to facilitating the access and intensifying the enjoyment of the culture, the knowledge, and the entertainment throughout the world.

3. European Union legal framework on Intellectual Property: Principal References

3.1. EU Directives

3.1.1. Directive 2001/29/EC, on the harmonization of certain aspects of copyright and related rights in the Information Society

With the objective of adapting the related legislation to copyright and related rights to the technological changes and especially to the mentioned Information Society, the Directive 2001/29/EC, of the European Parliament and of the Council, of 22 May 2001,

Intellectual Property Rights and Copyrights

on the harmonization of certain aspects of copyright and related rights in the Information Society (Directive 2001/29/EC), was published.

Additionally, the Directive 2001/29/EC aims to adapt to the EU context, the principal international obligations derived from the two copyright and related rights treaties passed by the World Intellectual Property Organization (WIPO) in 1996:

- WIPO Copyright Treaty
- WIPO Performances and phonograms Treaty

This objective, to transport or adapt the legislation of EU countries to the cited Treaties of the WIPO, finds this chapter skating the most relevant criteria to determine those points to consider regarding this material and the possible implications with respect to deploying the new Protocol IPv6.

With regard to the WIPO Copyright Treaty and always stressing the most relevant aspects for the objective of this Chapter, the following must be highlighted:

- The countries that seek to comply with the Treaty should establish the adequate legal protection and use the effective legal resources in order to avoid all actions that intend to escape the technological means used by the authors with respect to their works, with the aim of offering corresponding protection granted by this Treaty or for the Berne Convention for the Protection of Literary and Artistic Works.
- Furthermore, legal resources should be distributed to be able to direct against any person who, with knowledge of the cause, executes determined acts that introduce, permit, facilitate, or hide an infraction of any of the rights outlined in the Treaty or in the mentioned Berne Convention. Examples of such acts could be the following:

  a. Remove or alter, without authorization, any electronic information regarding the management of rights. In accordance with the Treaty, this information should be understood as 'information regarding the management of rights', such information that identifies the work, the author, the holder of any rights to the work, or information about the terms and conditions for using the work, all the numbers or codes that represent such information, when any of these elements are attached as a sample of a work or form part of its public communication.

  b. Distribute, import for its distribution, send or communicate to the public without authorization simples of works realizing that the electronic information regarding the management of rights has been removed or altered without authorization.

With respect to the WIPO Performances and Phonograms Treaty, it must be stated that the fundamental aspects in regard to this present Chapter, coincide almost entirely with

those in relation to the WIPO Copyright Treaty. In specific, the following is established:

- In relation to the technological measures that interpreters or performers or phonogram producers seek to establish in order to respect their rights, the countries that desire to comply with the Treaty should distribute the adequate legal protection and effective legal resources against the elusive actions of such measures.
- In addition, distributing of the following is an important aim: adequate and effective legal resources against any person who, with the knowledge of the cause, executes acts that infringe upon the rights or, with respect to the same, there exist reasonable motives to know that induces, permits, facilitates or hides an infraction of any of the rights mentioned in the Treaty. In short, the infringement acts could be the suppression or alteration, without authorization, of any electronic information about rights management or the distribution, emission, communication making available to the public, without authorization, of interpretations or performances, samples of interpretations or performances fixed or phonograms.

Returning to the Directive 2001/29/EC, the regulated contents of great interest according to the present Chapter coincide, almost entirely, with those expressed in the WIPO Treaties.

It is interesting to reiterate what is stated in the Preliminary Consideration (55) of the legislation and the relation to the information that aids in rights management:

- The greatest efficiency for distributing works that take into account the advanced Technologies is accompanied to the holders of the distributed works, with the necessity to better identify the work or rendering of such, the author, the right holder, and distribute information over the conditions and modes of use of the work or rendering with the aim of simplifying the management of rights.
- In addition, it is suggested that it must be 'indicated' to the right holders the use of 'marks' which refer, apart from the information about rights management, between other things, the adequate authorizations, when the protected Works are included in telematic networks.
- It is necessary to establish legal protection, harmonized at EU level, intending to avoid actions that may remove or alter the information for the electronic management of the author's rights linked to the work.

Considering the articles of Directive 2001/29/EC, article 6 highlights, in summary form, the following items:

- An adequate legal protection will be established against the elusive acts using technological measures adopted for the protection of the author rights.

Intellectual Property Rights and Copyrights

- An adequate legal protection will be established for the fabrication, importation, distribution, sale, rent, publication for sale or rent, or possession with commercial aims of any device, product or component or rendering of the following services:
  a. Promotion, publicity or commercialization with the aim of eliminating technological protection measures.
  b. Such promotion of technological measures will only hold a limited commercial aim.
  c. That it is principally conceived produced, adapted or executed with the aim of permitting or facilitating the elimination of the technical protection measures.
- 'Technological measures' can be defined as all techniques, devices or components that, while normally functioning, are destined to interfere or restrict acts referring to works or protected rendering of services that are not a part of an authorization by the right holder on the copyright or the related rights. The technological measures are considered 'efficient' when the use of a work or protected rendering of services is controlled by the right holder by means of the application of an access control or protection procedure, for example, encoding, randomizing or other transformation of the work or mechanism for controlling its reproduction, such an aim of this protection.

Considering article 7, it establishes the norms with respect to the 'Obligations related to the information for rights management'. In brief, this article comes to articulate the following:

- It should be established an adequate legal protection facing all persons that, knowing they execute without authorization determined acts, knowing or having reasonable motives for knowing that upon completing such acts induce, permit, facilitate or embody a violation of copyright or the related rights. The vulnerable acts would be similar to those determined in previous sections of this Chapter.
- 'Information for the management of rights' is defined as all the information provided by the right holder that identifies a work or protected rendered service by the author or any other rightful claimant, or information regarding the conditions for using the work or protected rendered service, such as any number or code representing such information.

3.1.2. Directive 2004/48/EC, on the enforcement of Intellectual Property Rights

The Directive 2004/48/EC, of 29 April, on the enforcement of Intellectual Property Rights, states the following additional objectives within the European Union:

- Obstruct the losses within the market as well as for companies that piracy produces. These losses can assume a disestablishing factor for the markets due to, for example, in the case of multimedia products, the usurpation of a trademark and the piracy of Internet do not cease in increasing and creating, as a consequence, substantial losses.

Intellectual Property Rights and Copyrights

- Fight for the protection of the consumers with regard to the usurpation of the trademark and the piracy that normally accompanies achieving to deliberately deceiving the consumer with respect to the right to wait and specific level of quality of a product.

From a general point of view, with these objectives, the Preliminary Considerations of the norm that can result as of interest to the present Chapter would be the following:

- The Preliminary Consideration (2) indicating that even though Intellectual Property should permit that an inventor or creator obtains a legitimate profit from his invention or creation, as well as permission to disclose as much as possible the work, ideas and new knowledge, that does not serve as an obstacle for the free circulation of the information, including in Internet.

  It is necessary to obtain a balance between the copyright protection of the contents transmitted and the right allowing such information to circulate freely. If this balance seems simple from a theoretical point of view, in practice and with the existence of potent diffusion means like those found in Internet, serious difficulties arise as to controlling copyright protection, for example, with the massive exchange of music and video through P2P applications. In this context, the objectives of this Chapter can be seen, aiming to establish in which measures IPv6 can aid in 'fighting' the acts against Intellectual Property, for example, piracy.

- The Preliminary Consideration (14) defines the 'acts executed at a commercial level' as those acts executed by obtaining economic profits or direct or indirect commercial negotiations, excluding, normally, those acts executed by the consumers of good faith.

- The Preliminary Consideration (20) reflects the importance of evidence as a fundamental element to test the infractional acts towards the IPR, indicating that it is helpful to guarantee the availability of means of presentation, collection and protection of evidence.

- The Preliminary Consideration (21) describes the Right to information as that which permits obtaining precise data about the origin of the goods or litigious services, the distribution circuits and the identity of whatever third person implicated in such acts.

Considering the mentioned norms, it is relevant to state that article 1 indicates the use of concept IPR to include Industrial Property rights.

For its part, articles 6 and 8, relating to the 'Evidence' indicate, in brief, the following:

- Without prejudice to the confidential data, in the case that the part presenting evidence reasonably available and sufficient for the rebuttal of allegations, to base the allegations that other evidence find under the control of the contrary side, the judicial authorities can order that the contrary side deliver such evidence.

- In terms of part that have presented reasonable available evidence for rebutting the allegations, rapid and efficient means can be outlined to protect pertinent evidence with respect to the supposed infraction, without prejudice that it is necessary to guarantee the protection of all confidential information.

In this sense, IPv6, technically, could provide more precise test mediums than those contributed by the previous version IPv4, for example, in the way of identifying the participants in a transmission of information.

Considering the right to information, article 8 of the Directive indicates that, in the context of the procedures relative to an infraction of the IPR and as a response to a justified and proportionate claimant, the judicial authorities can order to disclose the data regarding the origin and the distribution networks of the goods or services infringing IPR regarding the offender or any other person that has been found, on a commercial scale, in possession of the contentious goods or having used contentious services.

In relation with this point, it becomes frequent that the national legislation of some Member States consider a retention debt for the traffic of data in the electronic communications field, for example, the data related to the IP´s participants in communication, logs, data about transactions, etc., which is possibly the best performance of those demanded by the mentioned article 8 of the Directive, and as such converts into a medium to effectively execute the persecution of damages to the IPR's.

3.2. Council Regulation on the Community Trademark

The fundamental norm in Community trademark with respect to regulation of trademarks is the Council Regulation (EC) nº 40/94, of 20 December 1993, on the Community trademark, which seeks to create a trademark applicable to a communal scope.

Within this legislative base, a system is established to permit the granting of community trademarks by the named Office for Harmonization in the Internal Market. Through a petition solely presented before the OHIM, the community trademark takes on a unitary character in the sense that it produces the same effects within the assembly of the European Community.

All signs that can be considered graphic representation objects can constitute as community trademarks, always when these signs distinguish the products or services from one company to another.

Community trademarks award holding an exclusive right in such a manner that the right holder may prohibit a third party from using such trademark for commercial ends such as the following:

- A sign identical to the EU trademark for identical products or services that were registered with such a trademark.
- A sign creating confusion for the public in distinguishing it from the trademark.
- A sign identical or similar to the EU trademark for products or services that are not similar to those holding the EU trademark when the use of the sign thus takes advantage of the prestige or distinctive character of the trademark.

Conversely, the right granted by a community trademark does not permit the right holder to prohibit a third party to use the following information for commercial ends:

- Name and address.
- Indications relative to its species, quality, destination, value, geographic origin, moment of the product or rendered service's fabrication and their characteristics.
- The trademark, when this use necessary to indicate the destiny of the product or rendered service, in particular, as accessory or spare part.

3.3. Proposal for a Council Regulation on the Community Patent

With the aim of creating a new unitary title for Industrial Property in order to eliminate the obstacles for free circulation of the products in the internal market, the Commission Proposal has drafted on the 1st of August 2000, the Council Regulation on the Community patent.

Currently, there exist within the scope of the European Union two methods of guaranteeing the protection by means of patents: the national systems of patents and the European system of patents, highlighted in the Assembly, 5th of October 1973, on the Granting of Patents in Europe patents, better known as the Assembly of Munich.

In spite of this Convention creating a unique system of granting patents, there still does not exist a community patent that forms part of the series of legal EU norms.

The aim of the Proposal for a Council Regulation on the Community patent is not to substitute the existing national and European systems, but to be added on them. Consequently, the applicants must choose the option they want to follow.

However, the principal idea of the Proposal is for the Council Regulation to comply with the Munich Convention. As such, the granting conditions of a patent are obtained, for example, by means of this Convention.

A community patent grants to its holder the right to prohibit the following acts on behalf of any third party that lacks his consent:

- The direct exploitation of the invention, as well as fabricating, offering or introducing it into the market, importation, etc.
- The indirect exploitation of the invention.

The use of a patent by a person other than the right holder is outlined by a system of licenses, those that can become obligatory, for example, for a lack of or insufficient use of the community patent.

4. Situation of Intellectual Property Rights in the Electronic Scope

Upon analyzing the most relevant aspects of the community legislation with respect to Intellectual Property, this Chapter is centered, in this section, on reflecting which are the principally problematic elements of this material in the scope of electronic communications and Internet.

The main development of electronic networks for transmitting information – Internet and electronic mail being the two most widely-used aspects of this phenomenon – along with the development of electronic support for data in its various forms has provoked, on one hand, new methods of using the IPR and, one the other, the destructive effect of the rapid increase in ways to violate such IPRs.

In responding to these violations of IPR that currently take place within the electronic scope and to be able to analyze if the use of IPv6 can serve as a medium for eliminating or minimizing of such violations, it must be brought to light two of the most frequently violated rights: Copyright and Trademark.

Considering Copyright, the violations by means of electronic mediums are well known, but the following are examples to be reiterated:

- File exchange in P2P networks without authors' permission and without payment of the corresponding retributions.
- Promotion, distribution and utilization of techniques to suppress or disable the anti-copy systems of certain files, incorporated or not into the digital support.
- Piracy of music, software, games, and in general, contents protected by Intellectual Property, through its purchase, rent, etc., through the Internet.
- To take into possession contents (texts, photographs, audiovisual files, etc.) published on Internet without an author license or exceeding the granted license.

In relation to Trademark, within the principal examples of violations by means of electronic means, it makes sense to highlight the following examples:

Intellectual Property Rights and Copyrights

- Vulnerability in practice, in many cases, supposes disloyal competition, which occurs in occasions with the contents of certain indiscriminate deliveries of email messages not wanted, or spam.
- Phishing, a technique that consists of attracting a user, by means of deceits, to a fraudulent website where the user is open to introduce personal and private data. In both cases, the fraudulent website utilizes objects susceptible to trademarks, rights held by companies or entities that seek the same status.
- Spoofing, a technique to simulate or usurp the identity of an element in the network (personal computer, server, router, etc.), whose identity had been previously obtained in order to gain access to the resources of a third system, access that is based on confidence in the system accessed that has as an element a substituted network. Logically, the techniques of ascertainment and impersonating the identity can include, in many cases, the violation of copyright upon using trademarks or objects susceptible to protection that are right holders, for example, for the entity whose system was accessed.

Finally, within the scope of Patent rights, violations of these rights produced by means of industrial espionage attacks remain important to consider, especially those that are carried out by Internet (by means of unauthorized access, techniques of sniffing, communication interception, etc.) as mediums for arriving to patented inventions or patented companies.

Certainly, the technological elements are in constant evolution and progression, which permits a constant improvement of networks, services, applications, etc. One clear example is the continuous increase of the ability to transmit large quantities of data at a fast rate. However, this evolution gives rise to an increase in the risk of transmitting contents susceptible to IPR as well as an increase in the volume of contents transmitted infringing upon the applicable legislation.

Facing this situation of 'double use' of some advanced electronic communication technologies, articulating what role IPv6 may have seems relevant in order to avoid, or at least, diminish the number of behaviors that are infringing upon the Intellectual Property legislation.

It is true that the Protocol has not been developed with the aim of promoting the protection of the IPR, but it is no less true that its aim is a development that secures the adherence to the legislation and that, given it comes under criteria of optimization, its parts implicated in its development are in accord, etc., it can group characteristics that avoid or diminish the contradictory acts towards the Intellectual Property legislation or permit a better evidential response and legal confrontation to these acts.

Intellectual Property Rights and Copyrights

5. Influence of IPv6 in the scope of Intellectual Property Rights

It is well known that the Euro6IX Project has the principal objective of supporting the rapid introduction of IPv6 in Europe. From this, a series of results have been defined that, among others, become the design and deploy for the network until the complete development of the end-user services.

The development of the Euro6IX Project includes the disclosure of networks, advanced network services, applications, etc., that can be tested by the partners of the Project or by other groups of users or even by third parties interested in intervening as to the results of the Project, always under academic investigation watch, non resulting in achieving, initially, in commercial ends.

Definitely, the Project seeks to attain developments and tests for the participants elements in each one of the necessary levels in order to introduce IPv6, logically coinciding with the development of services and applications that, normally directed to end-users, are going to be utilized in some cases for the transmission of contents susceptible to the protection by IPR. Thus the protection and management of such rights is a factor that should be kept in consideration during the use of the implemented services and applications.

From this point, it is interesting to highlight a brief summary of the types of communication addressing that are defined in IPv6 with the aim of carrying out the transmissions of information and controlling what and who is doing such transmitting. From this, the types of addresses that are trying to be established are the following:

- 'Unicast. This group of addresses is characterized by identifying only one point of final destination (point-to-point). Any content sent to a unicast address will be delivered to only one destination point.
- Multicast. Multicast addresses are made up of a set of final destination points. Any content sent to a multicast address will be delivered to a set of destination points that form part of the same group.
- Anycast. This group of addresses, as with multicast, is made up of a set of final destination points. The principal difference is the delivery system of datagrams. A datagram sent to an anycast address is delivered only to one destination point (the closest one of the group at the time of delivery)'(5).

Under these premises, a series of applications and services are being developed resulting in a common use or transmission of the contents, data, etc. susceptible to the IPR whose ownership may not correspond with the participants in the telematic communication. Concretely, some of the services and applications through which contents susceptible to IPR

(5) 'El protocolo IPv6 y sus extensiones de seguridad IPSec', Verdejo Álvarez, Gabriel. Universitat Autònoma de Barcelona, febrero 2000

can be utilized or transmitted are the following examples: P2P, videoconferencing, on-line games, streaming (audio and video or just audio), VoIPv6, Chat/IRC, Messengers, email, customized services or services on demand, television and digital video, etc.

In such a way, although it is evident that IPv6 does not orient its development specifically towards the management or protection of IPR, it is without a doubt that the Euro6IX Project is a clear example showing that the developments made with relation to the Protocol, defining not only the form of addressing but also the networks, advanced network services, applications, etc., can come to influence the form of protection of these rights. In the same way that the definition of IPv6 has strived to keep under consideration the legal aspects related with privacy and the processing of personal data, it is equally important to consider that within the elements forming IPv6, there exist some like IPSec that can hold special importance in the configuring of the mediums in order to obtain control over the management and use of the IPR applicable to the transmitted contents, provided its conformity with the legislation analyzed in the previous sections of this Chapter.

6. Security at the Service of Intellectual Property

Given the strong business competitiveness in all sectors and levels across the world, Intellectual Property protection of strategic information and new products, including protection of the very image of a company, obligates the adoption of a series of measures for controlling access and the confidentiality. This makes the implementation of reliable security systems increasingly essential.

It is for this and other reasons that the information security, in general, receives a fundamental part in the development of the Euro6IX Project. What is more, the security is considered as an element integrated into the Project, expressed through the Protocol IPSec, configured as an intrinsic requirement of IPv6.

6.1. Approach to the Questions Relative to Internet Security

Firstly, the concept of security must be understood as a widely used term with the objective of covering all the threats, physical and/or logical, that affect each one of the elements such as transmitters or receptors that, under whatever conditions, intervene in Internet.

With this said, it is crucial to highlight the fact that the Protocols utilized in Internet (to establish the communication between the participants for the transportation of information, etc.) do not possess as an intrinsic characteristic the establishment of determined parameters of security. Because of this, the advancement in the use of Internet and the growth of its social and economic importance is accompanied by the parallel increase in the vulnerabilities (understood

as risks that affect the communications, the subjects of such communication or the contents being transmitted), which search to take advantage of weak zones that produce errors in the security of traffic in the Internet.

Without covering technical aspects of the methods for stopping attacks or violations of the vulnerabilities in Internet, it remains to be stated the examples of tests to the Internet, such as the following:

- Physical or logical intrusions about the elements by means, which the communication is executed.
- Virus attacks, worms, Trojans, etc.
- Spoofing or hiding the identity of a person, physical or legal, with the aim of regaining information or accessing resources without due authorization, etc.
- Violation of the communication confidentiality.
- DoS (Denial of Service) attacks, manipulation of information by intermediate persons.
- Violation of IPR(6).

It is confirmed that the security was not an original requirement for Internet, but it comes as an added element as a result of the necessity for tools of elimination or minimization of the weaknesses in Internet.

6.2. IPSec: The Element of Security for IPv6

'IPSec is a standard that seeks to distribute security services to the IP level as well as to all the superior protocols based on IP (for example, TCP y UDP)'.(7)

Regarding the utility of IPSec, from the point of view of the analysis put forth within this Chapter, it is necessary to mention that IPSec, in sum, authenticates the devices implicated on a transmission of information, and, with the configuration established, can come to cite such information for its proper transmission between hosts located in the network (Internet, intranet, extranet, etc.), including those communications established between a server and a terminal, a client or workstation, and between servers. Security at the IP layer distributed by IPSec aims to provide protection to the IP packets. The IPSec Protocol is based in an end-to-end security model, such that only those sender and receiver points of the network should be compatible with the Protocol and should accept the protection of the transmitted information.

The Protocol IPSec comes being utilized (for example, in the creation of Virtual Private Networks o VPNs) with the version 4 of the Internet Protocol (IPv4), but as an additional

(6) 'IPv6 y la respuesta a la muerte de Alice', Gómez Skarmeta, Antonio F. Departamento de Ingeniería de la Información y las Comunicaciones de la Universidad de Murcia, febrero 2004
(7) 'Análisis del protocolo IPSec: el estándar de seguridad en IP'; Pérez Iglesias, Santiago. Revista 'Comunicaciones de Telefónica I+D', noviembre 2001

part. However, in the case of IPv6, the Protocol IPSec has been established as an intrinsic or mandatory element for development and implementation, with which the version 6 of the Internet Protocol supplies the greatest level of optimization for security.

In addition, the Protocol IPSec, designed to function in a transparent mode within the existing networks, accounts, among its other advantages, the fact of 'having been developed with support from standards of Internet Engineering Task Force (IETF)'(8), an international group of experts linked to the evolution of Internet architecture and its optimum performance(9). The results of different expert team activities are reflected through the Request for Comments (RFC).

On the other hand, besides the advantage of the intervention of IETF in the development of the Protocol and even without entering into a description of the performance of the Protocol, it is possible to attribute a series of advantages of the proper Protocol IPSec, which would be, in brief, the following:

- As already mentioned, it is included in IPv6, whereas in the Protocol IPv4, integration is a mere optional possibility. The obligation to implement IPSec in all of the IPv6 nodes permits that, upon establishing an IPv6 session, it is always possible to dispose a safe end-to-end connection.
- Distribute a common and homogenous security level for all of the applications.
- It is independent of all the physical technology employed.
- It is compatible with public key infrastructures (PKIs).
- It is implemented in a transparent mode within the network infrastructure.
- It is an open standard of the sector in order to distribute private and secure communications. As a result, it is also a standard for achieving privacy, integrity, and authenticity. The authentication and the encoding of the data for their protection from other terminals make safe transactions over IPv6 possible. As such, for example, the Protocol IPSec could be used as a tool that would serve not only for identifying the destinations of the transmission of contents protected by IPR, but also, by means of encoding, the interception by third parties of contents would be avoided, including the resend to an illegitimate third party.
- It is permitted to assume the increase in 'named' devices in other words, those devices that gather characteristics of mobility and possibility for connecting different types of networks.

(8) 'Análisis del protocolo IPSec: el estándar de seguridad en IP'; Pérez Iglesias, Santiago. Revista 'Comunicaciones de Telefónica I+D', noviembre 2001
(9) http://www.ietf.org

Intellectual Property Rights and Copyrights

6.3. Description of the Protocol IPSec and its Fundamental Components(10)

In this section, the technical aspects most relevant to IPSec will be analyzed in brief in order to facilitate the comprehension of the possibilities its adoption would conjure from the perspective of protecting the IPR.

IPSec, as an expression of its open character and its strength in being independent while confronting concrete encoded algorithms, is a set of standards for integrating in IP security functions based in cryptography. It distributes confidentiality, integrity and authenticity of datagrams IP, mixed with public key technology (RSA), encoding algorithms (DES, 3DES, IDEA, Blowfish), hash algorithms (MD5, SHA-1) and digital certificates X.509 v.3.

The tendency towards neutrality with respect to the algorithms utilized has resulted in IPSec being designed in modulate form, such that the set of algorithms desired can be selected without affecting the other parts of the implementation. However, the problems of inter-operability that could take place in Internet have resulted in defining certain standard algorithms that should support all the implementations that are performed. In this manner, the reference-encoded algorithms are DES and 3DES, as well as, MD5 y SHA-1, as hash functions. It is possible to use other algorithms that are considered safer or more adequate for the specific situation.

Within IPSec the following fundamental components are distinguished:

- Two Protocols of security: IP Authentication Header (AH) and IP Encapsulating Payload (ESP), which distribute mechanisms of security for protecting IP traffic.
- A Protocol for managing keys: Internet Key Exchange (IKE), that permits two nodes to negotiate which keys to use and all the parameters necessary to establish an AH or ESP connection.

The Protocol AH is used with the aim of guaranteeing the integrity and authenticity of the IP datagrams. In more detail, it distributes a medium to the sender of the IP packs in order to authenticate the origin of the data and to verify that that data have not been altered in their transmission. However, among its characteristics, there is not one that is directed towards distributing transmitted data confidentiality. The Protocol AH is a master in authentication that is inserted between the standard IP header (IPv4 as well as IPv6) and the transported data.

The performance of AH is based on the algorithm HMAC (Hashed Message Authentication Code), a message authentication code. This algorithm consists of applying a hash function to the combination of data between the entrance and the key, thus being a small chain of exits of determined 'extract' character. This extract has the capability of acting as a personal footprint associated with the data and the person that generated such data, provided that it is the only person who knows the key.

(10) Based on the article 'Análisis del protocolo IPSec: el estándar de seguridad en IP'; Pérez Iglesias, Santiago. Revista 'Comunicaciones de Telefónica I+D', noviembre 2001.

Intellectual Property Rights and Copyrights

On the other hand, the Protocol ESP aims to distribute confidentiality. With such an aim, it specifies the mode for encoding the information that is wished to be sent and specifies how this encoded content is included in the IP datagram. In combination with a similar mechanism to that of the Protocol AH, the Protocol ESP seeks to offer services of integrity and authentication of the origin of data.

The function of the code within the Protocol ESP is redeemed by a symmetric key encoded algorithm. The transmitter receives the original message, codes it using a determined key, and includes it in an IP pack, following the header ESP. During the transition to its destination, if the pack is intercepted by a third party only, it will obtain a set of unintelligible bits. In this case, the receiver will apply a new algorithm coded with the same key, recuperating the original data. As it can be easily seen, the security of this Protocol resides in the robustness of the encoding algorithm. In other words, an attacker cannot decode the data without knowing the key, just as the key ESP is known only by the sender and the receiver.

In terms of determining the utility with respect to the analyzed technical procedures in this section of this Chapter, it must be kept in mind that a hypothetical assumption could be, for example, the case of a record company that seeks to send contents of its musical catalogue by Internet. Through these procedures, it could come to assure that those musical contents, protected by IPR, are received only by the users, those who have solicited and have paid a determined amount of money. In this manner, the record company would achieve the following:

- Confidentiality of the transmitted content by means of encoding.
- Precise selection of the destinations that are going to receive the contents.
- Contributing guarantees to the receiver that the contents are derived from the corresponding sender, which is authorized for the diffusion of such information.
- Integrity guarantee of the protected contents, avoiding modifications by a third party.

However, following the mentioned example, independently of the record company's capacity to achieve the set aims using the protocols set forth in IPSec, it is no less true that these advantages won't separate from the concrete transmission of the referred contents, in this case, the transmission of the musical files. IPSec, and consequently IPv6, would not enter into the definition that the applicable legislation established for what is considered a medium of technology for the effective execution or protection of the IPR. As such, it is not possible the restriction of possible retransmission to unauthorized third parties of musical files or its transmission through a network P2P.

However, in spite of not capturing the concept of customized technology for the protection of IPR, IPSec would be considered an evidence of great value in many cases of violation of such customizations made in Internet, if each one of the telematic transmissions that damages those rights is considered.

Intellectual Property Rights and Copyrights

Moreover, the fact that the IPSec is not configured like a customized technology as was expected does not suppose that, with the appropriate technical and legal plans, it will not become such a technology. Proposing such a hypothesis would end in the possibility of incorporating determined information distributed by IPSec to downloadable information files (i.e. music, video, etc.) by Internet with the authorizations, licenses, etc. that would have determined the holders of the applicable rights, in such a way that the mentioned information would serve as the following:

- Determine which devices, identified by their IPs, could access the transmitted file.
- Determine if other devices, also identified by its IP, can have an authorized use (i.e. reproduction but not duplication) of the file or if the retransmission is prohibited to all persons who are not the original sender.

Consequently, the goal would be to articulate the systems managing the rights of contents through customized technology based in IPv6, and moreover, in IPSec. This hypothesis could be equally operative in systems of collective management, which could establish techniques of control based on the user identification according to its IP.

However, as a final note on the hypothesis mentioned, it must be considered that, to put it into practice, it would be necessary the study of technical and legal questions that are not part of this Chapter and, in the end, it could result in blending or limiting the possibility of some mentioned operations.

Returning to the description of the Protocols used by IPSec, it is evident that the distribution of keys in a secure form is an essential requirement for the success of the Protocols ESP and AH, as previously seen. Likewise, it is fundamental that the sender and the receiver are in agreement with the encryption algorithm or the hash as well as with the rest of the common parameters to be used.

This negotiation is carried out by a control protocol, named IKE, to be covered in more detail in the future, due to the fact that this Chapter remains to provide a brief reference to the two modes of procedures that permit the Protocol IPSec:

- Transport Mode. Using transport mode, the content which is being transported within AH or ESP datagrams, is data of the transport layer. Consequently, IPSec header is inserted immediately after the IP header and before the data of higher levels, which is desired to be protected. Transport mode has the advantage that it assures the communication end to end, but requires that both ends understand IPSec Protocol.
- Tunneling Mode. Using tunneling mode, the content of datagram AH or ESP is a complete IP datagram, including the original IP header. Thus, an IP datagram is taken and an AH or ESP header is inserted initially. Later, a new IP header is added and this

is the one that is used to route the packages through the network. Normally, tunneling mode is used when the final destiny of the data does not agree with the device that carries out the IPSec functions.

Once the data for the working methods of the IPSec is established, an essential concept to IPSec must be analyzed, such as Security Association (SA). This concept references a channel of unidirectional communication that connects two nodes through which the protected datagrams flows by means of cryptographic mechanisms previously mentioned. Once a unidirectional channel is identified, an IPSec connection is composed of two SAs, one for each of the addresses of the communication.

Until now, it has been assumed that both extremes of a SA should know the keys, as well as the rest of information necessary for sending and receiving AH o ESP datagrams. As previously mentioned, it is necessary that both nodes are in agreement with the cryptographic algorithms to be used as well as with the parameters of control. This operation can take place by means of a manual configuration, or through any Protocol of control that is in charge of the automatic negotiation of the necessary parameters, naming this operation like a SAs operation.

The IETF has defined the Protocol IKE (Internet Key Exchange) in order to achieve the automatic management of keys as well as an establishment of the corresponding SAs. An important characteristic of IKE is that it is a standard Protocol for key management.

In this respect, IKE is a Protocol hybrid as a result of the integration of two complimentary Protocols: ISAKMP and Oakley. ISAKMP (Internet Security Association and Key Management Protocol) define the Protocol of communication and the syntax of the messages that are used in IKE, while the Oakley specifies the logic of how a secure exchange of keys between two parties that do not know each other previously is achieved.

The principal objective of IKE consists of establishing a encoded and authenticated connection between two entities through which the necessary parameters are negotiated in order to establish an association of security IPSec. This type of negotiation is accomplished in the following two phases:

a. The phase in which both nodes establish a secure and authenticated channel. This secure channel is achieved by means of the use of symmetrical encoded algorithms and an algorithm HMAC. The necessary keys derivate from a master key obtained by means of the key exchange algorithm Diffie-Hellman. This procedure does not guarantee the identity of the nodes so that it is necessary to take an additional step in authentication.

b. There exist various methods of authentication, even though the two most commonly used are the following:

I. Authentication based on the knowledge of a shared secret. By means of using the hash function, each side demonstrates its knowledge of the secret without revealing its value.

II. Authentication based on using the digital certificates X.509 v3. The use of certificates permits the secure distribution of the public key of each node, such that it may test the identity of each by using the private key in possession and other cryptographic public operations. The use of certificates requires, logically, the previous establishment of a Public Key Infrastructure (PKI).

c. In the second phase, the secure channel IKE is used to negotiate the specified security parameters associated with a determined Protocol, in this case, IPSec.

d. During this phase, the characters of the connection ESP or AH and all of the necessary parameters are negotiated. The device that has initiated the communication will offer all the possible options configured in its security policy and with the priority with which they were configured. The receiver system will accept the first that coincides with the security parameters that are named. Likewise, both nodes are informed of the traffic that is going to interchange through the mentioned information.

As a final comment and conclusion to this present section, the following is an analysis of the characteristics of the security services that offers IPSec. These services are the following:

- Integrity and authenticity of the original information. The Protocol AH seems to be the most adequate if it does not require encoding.
- Confidentiality. The service of confidentiality is obtained by means of encoding included in the Protocol ESP. This Protocol also contains tools for masking the type of communication that is in process.
- Detection of repetitions. The Protocols ESP and AH incorporate a procedure in order to detect repeated packs. This sequence cannot be modified by the attacker due to it being found protected by the option of integrity for any of the two Protocols (AH and ESP) and whatever modification of this number would provoke an error in testing the integrity of the pack.
- Access control: Authentication and authorization. Given that the use of ESP and AH require the knowledge of keys, and such keys are distributed by means of an IKE session in which both nodes are authenticated mutually, there exists the guarantee that only the desired parts participate in the communication. The valid authentication does not imply a total access to the resources, due to IPSec also provides authorization

functions. During the negotiation IKE the flow of IP traffic, which will circulate through the IPSec connections is specified.

- Not repudiation. The service of not repudiation is technically possible in IPSec, if an IKE with authentication is used by means of digital certificates. In this case, the authentication procedure is based in the digital signature of a message that contains, among other data, the identity of the participant. This digital signature, because of the existing link between the public key and the identity that guarantees the digital certificate, is an unequivocal evidence that an IPSec connection has been established with a concrete device, so this one will not be able to deny it. Actually, this proof is more complex, since it would require to store the IKE negotiation messages and, in addition, currently it has not been defined a procedure to link this with a concrete date.

6.4. PKI

6.4.1. Description of the principal elements of a PKI

Under the name PKI (Public Key Infrastructure), the technical elements and the administrative processes are grouped, those necessary in order to carry out necessary operations for sending and revoking certified by an electronic digital signature, and additionally renewing certificates and whatever other similar operations achieved using PKI. These operations are carried out for a community of subscribers, that is, the designees in the certificate.

The opportunity to dedicate a section of this Chapter to the typical structure of a PKI is due not only to the fact that the identification of participating nodes in a communication using IPSec could be done with digital signature certificates, as it was said. The opportunity arises because the utilization of these certificates could join characteristics of such certificates with those of IPSec, either on its own or reinforced.

In this manner, the creation of PKIs based on IPv6, as they currently come tested through the Euro6IX Project, it is a very interesting possibility, considering this type of structure posses the aim of creating a reliable system based in the unequivocal identification of the parts and in the possibility of customizing configurations of the grade of control and the confidentiality hoped to be granted to the transmission of the contents.

In the case of this chapter, which is determining the proper elements based in IPv6 that could be utilized for seeking the maximum respect to the Intellectual Property legislation, the advantages of using a PKI can be explained through a practical example: a company that would want to distribute contents protected by IPR (movies, music, electronic books, video on demand, etc.) through the Internet, taking advantage of the improvements to bandwidth

Intellectual Property Rights and Copyrights

that IPv6 can produce, an digital signature system could be considered for use according to the following functions:

- Make possible the identification of the contents receivers by means of a procedure of identification as well as delivering an electronic certificate that should be executed by identifying it before using the services for access to the contents.
- Permit guaranteeing that access to contents by third parties is impossible during distribution (i.e. by means of encoding) as well as beforehand, due to possibility of establishing that only persons disposing of the certificate can access these contents.
- Creation of a secure and controlled channel of distributing audiovisual contents for certain social sectors (i.e. minors) seeing as how a strengthened system of identifying those persons holding certificates can be determined which avoids the possibility of reaching the members of vetoed sectors.

Once the characteristics of a digital signature system or PKI can be seen, these can be utilized towards the aims of this chapter as well as for strengthening the characteristics that IPSec can hold, thus calling for a brief reference to the principal elements that determine a PKI.

The principal organ of the PKI, at a level responsible for the principal operations executed, is the Certification Authority (CA), which is responsible for the management and distribution of the certificates. However, it is also possible that the same PKI integrates with various CAs, structured through a hierarchical system of interdependency, in such a way that a Root CA is going to exist, under which other various hierarchical scales exist, occupied by the remaining CAs. Thus, there could be relations of hierarchical dependence also between the different scales. The interconnection and the hierarchical dependency between the CAs are maintained during the entire life cycle of the certificate, provided that its use requires validation of the certificates for all the CAs superior to the issuer CA.

The CA also is responsible for establishing the technical elements and the personnel necessary for executing the PKI. However, the CA can solicit the help of external companies, usually other CAs, so that they can provide technical elements and the necessary personnel for the PKI operations. This decision does not undermine importance to the role of the issuer CA, but only distributes the operations of PKI. The CA aims to establish a technical structure and of personnel that provides liability to the PKI from the operative point of view as well as that of security of operations.

Usually, the complex administrative, technical, personnel, and security structures of a CA are reflected in the Certification Practice Statements or CPS, which is established as basic documentary support reflected in the efficiency of the CA and the life cycle of the certificates. On the other hand, the concrete aspects of the CPS can be developed through external

documents or, for example, through details related with security. An important point to state regarding these complementary developments are the Certification Practice or CP, which include details of the particular aspects of each type of certificate send by a CA.

In spite of the responsibility and the control of a CA regarding the relative operations of the certificates, it is possible that there exists an Registration Authority (RA), as responsible organ to execute the administrative processes related to the soliciting of certificates and activating the first phases of their delivery. The RAs can be organs of a CA or they can be independent third entities.

On the other hand, descending to the most common levels of certificate use, the Applicant is the first figure to be outlined as an entity that manifests its capacity to endow him with a certificate sent by a CA in question, and indicates the steps of petitioning established. It is logical that the CA establishes a series of previous criteria that the certificate applicants should complete so that their obligations are fully understood.

The following figure or element to consider with PKI comes from the Applicant once the necessary requirements are checked and the process of solicitation is completed, the certificate obtains the status of Subscriber, in other words, holder of the issued certificate. With this status, the certificate Subscriber could use such certificate under the terms established in the CPS and the contract that has been drafted with the CA, and it will assume the corresponding obligations derived from these documents.

Finally, the last figure to outline is the User or Relying party, which would be that entity that, as destination of the certificate and by its own decision, decides to conform with it. In a way to assure beforehand the confidence of the received certificate, the User should have accepted the contract which establishes the terms of use of the certificate and, on the other hand, the CPS of the sender CA, in order to establish the terms by which the confidence is established and the roles, obligations and responsibilities of each part (CA, subscribers and users).

6.4.2. Possibility of Integrating IPSec with a PKI

The possibility of using a PKI within the electronic communications used by the Protocol IPSec is seen as a potential solution to the necessity for a procedure to authenticate a group of nodes seeking transmission by IPSec, thus being a very numerous groups of nodes.

The PKI is outlined by a hierarchical organization in which the operations of its subscribers is organized, which certainly positions an advantage to this option, permitting granting uniformity to the criteria of the decision and avoiding the insecurity that could result from the dispersion of the decisive elements. In this sense, it should not be overlooks that a PKI is based on reliable factors in balance with the participants.

Intellectual Property Rights and Copyrights

In the case of IPSec, the subjects of certificates, the subscribers, are going to be the proper IPSec nodes. The function of the certificates, in this case, is to distribute a reliable medium for authenticating the identity of the IPSec devices. Each one of the IPSec devices will contain a digital certificate that will possess a public key and sufficient information to identify the negative without error. This association between public key and identity is endorsed by the CA signature integrated in the PKI, which gives credibility to the certificate.

Even though the Protocols for the interaction of the IPSec devices with a PKI are not specified in any of the standards in which the technical aspects relative to IPSec are developed, it is habitual to use, in the currently operating PKI, the standard X.509 v3 as a common format for the certificates, as well as the standard of the series PKCS (Public Key Cryptography Standards) in order to solicit and distribute the certificates.

In general, the IPSec nodes necessary to execute certain basic operations with PKI are the following: access a certificate of CA, solicit and distribute the certificate, checking the credibility of the certificate received. Usually, the IPSec nodes provide the validation of the certificates by means of consulting the Certificate Revocation List that is stored in the directory of the PKI, even though there exist other forms of checking the validity of the certificates, such as OCSP services (On-line Certificate Status Protocol).

6.5. IPSec as a tool for assisting the protection of Intellectual Property

Even though the principal function of IPSec would not be the protection nor the management of the IPR that can recover the contents, data, etc. that circulates the Internet or, in general, is transmitted in electronic mediums, it seems possible to extrapolate certain elements of the Protocol to use it for protection or management of the IPR.

The existence of the public address attributed specifically to each point of the Internet, together with the modes of addressing used by the Protocol (multicast, unicast and anycast) permit a beginning level of control over the transmitted contents, seeing as how it is possible to determine the destinations and the uses of the information transmitted. For example, considering an end-to-end transmission of contents like a movie, aimed at unicast or multicast addresses, the following advantages could be obtained:

- Determining, in a precise and unequivocal manner, the IP addresses of the transmitted contents' destination.
- The identifying characteristics of IPv6 could permit a substantial improvement to the methods of managing the IPR, independently from the management of, for example, by the proper owner or, more commonly, by a Collective Management organization. In this manner, the retributions can be executed toward those right holders regarding the transmitted contents.

- Furthermore, the identification of the destination addresses permits that, in the case of contents discarded or captured by electronic means, these could only be utilized by the holders of the addresses authorized by the sender, for example, only those destinations that dispose of one of the IP numbers recovered as additional information within the protected contents.
- In the cases resulting from the illegitimate use of protected contents, the technical procedures for identifying the intervenient users could be improved, due to the fact that is could be improved, considering the case of Internet, each uses, node, or participating point would be identified by the IP.

Another additional part to the possibilities referred to is improving the use of IPv6 characteristics for managing and exploiting the IPR is IPSec is utilized, the element of intrinsic security for such acts.

The IPSec characteristics increase the innate possibilities of IPv6 at the moment of establishing the most rigid controls over the information flows that take place over Internet and that include contents susceptible to IPR.

In face of significant problems such as the exchange of files with vulnerability to the IPR through the P2P networks, or the vulnerabilities of trademarks or the damages in the usage of Internet as well as the usage of the technology means of companies that may involve spam, the flexibility that permits IPv6 and even with the functions of IPSec, this allows to obtain more solid mediums of tests before a hypothetical vulnerability of the Intellectual Property legislation. For example, in the case of detecting the transmission of music files without authorization by the IPR holders, it would be helpful to detect the source of the transmission as well as the receivers of the files they are illegitimately downloading.

Furthermore, it is not ignorable that one of the future uses of IPSec as a possible technique or electronic system for the protection or management of IPR, in such a way that no only would it secure and optimize the transmission of information with respect to the IPR, but also that the new Protocol can allow for the holders of rights to receive the corresponding retribution for the exploitation. In the case of Collective Management organizations, they could establish an electronic system of management based on the characteristics for determining the users that are given by the IPSec Protocol.

Finally, it must be reiterated the use of the Protocol IPSec for protecting the IPR, articulated through an additional technical step for addressing the transmissions or executed communications. This path would separate from the possibility of incorporating the addressing information that the IPv6 establishes and, in a secure mode, IPSec, to the proper data or files transmitted. In this way, the control over the destinations permitted by the new Protocol is extended, in this case, to the life cycle of the transmitted information, possibly

articulating it as control mechanisms for the 'illegal' use of information by the transmission by telematic mediums (i.e. exchanges in a P2P network), by its incorporation to a physical support. In this last case of incorporation to a physical support, if the information about the sender is added, it could be checked if, beforehand, this source had the authorizations, permits or licenses necessary to execute such an action or, for example, it had a previous illegitimate elimination of the mediums of protection for the files that could have been established by the holder of the corresponding rights.

6.6. IPv6 and Digital Terrestrial Television

Within development of the digital environment, the Digital Terrestrial Television (DTT) is one of its prominent advancements. The DTT is considered one of the best improvements within the scope of electronic communications which permits an enormous extension of the capabilities to transmit contents susceptible of IPRs, as under IPv6.

Consequently, it is possible to consider the fact that a technological integration between IPv6 and DTT could result in important advantages, for example, regarding the protection of contents under IPRs.

Although the main target of IPv6 is not the protection and management of the IPRs, there are, however, some characteristic of the protocol that could help to reach a better protection of the contents susceptible of IPRs.

In addition, the use of IPv6 could also have legal consequences for the parties that take part in the emission of the DTT, including the user or viewer.

Thus, it would be possible to highlight the use of the QoS or CoS techniques in the creation of the IPv6 packages used to provide DTT services. Since these techniques make possible the qualification of the information transmitted through packages generated from the IPv6 protocol, an agreement between the DTT operators would be needed (sectorial agreements, multiparty agreements, agreements generated by international organizations, etc.), by which the qualification rules, hierarchies of contents, people authorized to make the qualification, etc shall be determined.

Another example of how IPv6 could be used in the DTT sphere could be the possibility of establishing the necessary techniques in order to restrict the access by minors to certain types of contents.

The DTT operator could establish in the contract signed between the operator and the viewer that certain payable contents (i.e. pornography) will be linked to a concrete IP address which must belong to the viewer. This could be done basing the emission on the unicast method of IPv6. In such a way, the DTT operator could affirm that he has adopted all possible

measures in order to guarantee that the pornographic contents are accessed by a concrete user through a specific equipment identified by its IP. Therefore, there would be more guaranties that a non-authorized minor has not accessed to those contents.

On the other hand, other characteristics of IPv6 could be used to manage IPRs, in particular, to provide audiovisual contents on demand based on the user's profile. This profile would be associated to the IP address of the DTT viewer.

In brief, it could be possible to suggest the adoption of a payable audiovisual contents subscription contract, elaborated according to the following points:

- Contents shall be distributed by a multicast method to all the receivers identified by a specific Unique Identifier embedded in their IP addresses based on IPv6.
- The payment of the contents shall be made by one of the following formulas:
  - > Contents without publicity. The bidirectionality of communications in DTT allows managing payments without using a different channel (i.e. Internet or call-center).
  - > Contents and publicity. The user does not pay for the visualization of the contents, but he must accept the insertion of advertisement messages based on his profile which is associated to his IP address. The profile is created taking into account the use of the services integrated in the DTT platform that have been used by the user (thematic channels, electronic banking, trips, online purchases, leisure services, etc.).
- In this last case, the contract that regulates the access to payable contents shall contain the necessary obligations regarding the processing of personal data, as for example, informing the user about the processing of his data associated to his IP address based on IPv6. Also, obtaining the appropriate consent would be needed and achieved by either digital signature or a signature in writing.

In conclusion, the technological integration between IPv6 and DTT would allow to raise the possibility of taking advantage of the inherent characteristics of IPv6 in order to establish adequate legal relationships in the commercialization and use of the DTT.

7. Conclusions

The principal objective of this Chapter has been to study the possible implications and relations established between the new Protocol IPv6 and the related Intellectual Property legislation. One of the principal motives to assume this perspective derives from the realization that the electronic communications and Internet have converted into one of the most widely used means for committing damaging acts towards the IPR.

Intellectual Property Rights and Copyrights

Throughout this Chapter, IPv6 has been shown not to possess as its aim the protection of IPR nor the generation of formulas for such an aim. This is the cause for such an analysis as a result of the work done in this book in relation to the Protocol, the applicable legislation, the current problems for Intellectual Property in the electronic scope, the security protocol (IPSec) integrated within IPv6, etc. The focus has been from the point of view of determining the characteristics of the new Protocol that could be used for the protection and management of IPR.

It is necessary to reiterate, however, that not all the data, nor information being sent using IPv6 are going to be susceptible for the protection under the Intellectual Property legislation. For this reason, this Chapter has established those aspects most relevant to characterizing the types of data or contents transmissible and protected by the mentioned rights.

Apart from these initial objectives, the principal conclusions in relation to the possibility of extending the use of IPv6 and its security aspect, IPSec, within the scope of protecting and managing the IPR and, in general, for complying with the Intellectual Property legislation in the electronic scope or Internet are the following:

1. The design of IPv6 is being carried out considering and strictly respecting the legal framework that could be applicable towards its development as well as executing into practice. The legal implications must be considered to conclude if the uses of the networks, services, applications, etc that continuously are being developed, is possible.
2. The improvements in the electronic communications field, in constant evolution and progression like that destined for IPv6 have improved considerably the capacities to transmit contents susceptible to IPR. But the creation of new paths, the increase in cases of violating the IPR, is continuously increasing in volume.
3. The community legislation for Intellectual Property advances the creation of a legal framework for the elements for protection of the IPR. From this effort, the normative requirements are established for their implementation or evidence of violation, and it could be very important what role IPv6 takes with the security aspects of IPSec. Thus, for example, the measures of the community legislation where the positive influence of the new protocol can be seen as well as its security aspect being important to the enforcement of the technological measures that the holders of IPR can establish in order to protect their legitimate interests and those for the protection of 'information about the management of rights'.
4. The use of IPv6 can extend to the protection of the IPR. Even keeping under consideration that the new Protocol does not contain the aim of seeking tools for protecting and management of these rights, it is true that uniting certain characteristics, it could make possible its use in this manner. Among others, the function of identifying

the senders and receivers of electronic communication through the use of the IP number and the function of determining the legitimate destinations of protected contents, through the addressing typology established within the Protocol (unicast, multicast and anycast).

5. The use of IPv6 with the aim of seeking an improved management and protection of the IPR could improve in a substantial manner in the case of configuring the electronic communication with the utilities of IPSec, security protocols integrated in a necessary manner with the new protocol. In brief, the results of these conclusions, the use of IPSec as a tool for the management and protection of the IPR would give rise to the following advantages:

   a. Precise selection of the destinations for the protected contents.

   b. Confidentiality of the contents transmitted by means of its encoding.

   c. Granting guarantees of destination in relation to the contents sent by an authorized sender.

   d. Guarantee of the integrity of the contents.

6. In the same point of using IPv6 and IPSec as methods of protecting the IPR, it is possible to outline the possibilities of extending this function to the configuration of IPv6 and IPSec as technological means that the authors or holders of the protected contents could establish regarding their restriction on third party use.

7. The goal would be that IPv6 and IPSec are not used only to protect the contents during the addressing and execution of the electronic communication, but their use as a technological medium for protecting rights could arise from the fact of incorporating information created by the protocols for the proper transmitted contents (i.e. a music file), in such a manner that it would delimit the field of users and authorized uses with relation to the determined IPs and would impede, among other things, the illegitimate transmission of the content to third parties.

8. The relation between IPv6 and the protection of the IPR cannot be established in a direct mode due to the absence of characteristics of the Protocol especially destined for this aim. However, as seen throughout this Chapter, within those characteristics of the Protocol and within IPSec as its security aspect, there exists some characteristics that could improve the important method of management and protection of the IPR and that, in addition, could evolve to become technical tools specifically dedicated to the mentioned aims and, in general, to complying with the Intellectual Property legislation.

authors

authors

authors

Consulintel integrates networking and communications services and products.

Consulintel initiated its first steps with IPv6 when it was still not clear that this protocol would really become deployed in Internet. Today Consulintel is recognized worldwide as one of the leading companies, which has invested more resources in Research, Development and Innovation regarding IPv6. With expertise in many diverse aspects related to this protocol, the company has participated in numerous international projects and is heavily involved in standardization work.

Consulintel organizes a number of dissemination and training events related to IPv6. Among those, the Global IPv6 Summit, an international event, celebrated the fourth edition in June 2005, with the participation of the most relevant worldwide speakers.

ECIJA Ecija is a cutting-edge firm specialised in corporate and commercial law, offering multidisciplinary advice and high-quality integrated services.

According to The European Legal 500, Ecija is ranked as among the top 3 Spanish law firms in New Technologies. The firm is also listed among the top 30 firms in Spain and the first in Intellectual Property according to the Financial Times local counterpart, *Expansión 2003.*

Ecija maintains a strong client base for the IT sector, advising major Internet portals, telecommunications operators and software developers as well as public and private entities.

The firm relies on its qualified lawyers and professionals in order to deliver custom-made solutions, having a broad-ranged expertise in such areas as Corporate & Commercial, Dispute Resolution, Media & Entertainment, New Technologies and Intellectual Property.

The Department of Communication and Information Engineering from the University of Murcia UMU (Spain), has a significant experience in security in network infrastructure, security services, security in mobile devices, access control and smartcards developments. UMU has been participating in different national and international research projects, and establishing collaborations with important international research institutions, within its participations in several EU projects from the FP5 and FP6. Also UMU research group, has international collaborations with Latin America for PhD programs in different ICT areas like security, mobile services and middleware for pervasive system.

In the area of security UMU is actually involved in Euro6IX project in the FP5 and in SEINIT and POSITIF IST FP6 projects, working in different aspects as PKIv6 infrastructure, key management, secure signaling, Policy based Network Management and access control based on advanced protocols like PANA.

authors

Basar, Kaisor

Kaisor Basar studied law at Oxford University before attending the College of Law in Guildford. He qualified as a Solicitor of the Supreme Court of England and Wales in 1995 and worked at Lovells and Clyde & Co (top 20 law firm in London) before moving to Spain in 2001. He worked at Ecija Abogados from 2001 – 2003 as head of the international department and was involved in the Euro6IX project during this time.

Carbayo Vázquez, Francisco Javier

Javier obtained his law degree from the University of Cantabria and a Masters in New Technologies Law at Aliter Business School in Madrid.

Javier collaborates with the Data Protection and New Technologies departments as well as the IT division at Ecija, contributing to consulting work regarding the legal aspects for the development and implementation of IT projects.

In addition, he frequently participates with specialised magazines and publications, having written various articles about data protection, electronic signature, e-voting, electronic billing, the information society and legal aspects to consider for the development and use of information technology.

Écija Bernal, Álvaro

Alvaro obtained his law degree from the University of Madrid, Autónoma campus. He is a partner at Ecija Abogados.

His expertise includes Corporate & Commercial as well as New Technologies law. Currently, Alvaro is Project Manager and Legal-Technical Consultant for all projects within Ecija related to New Technologies and Data Protection. He led the European Union project 'Euro6IX' for the study and investigation of the IPv6 protocol and the legal data protection of such protocol users.

Alvaro has participated in various works such as 'The Audiovisual White Book' and 'Internet: Key legal aspects for businesses'. He has also written and coordinated such publications as 'Internet Contracts: Applications and Practical Suggestions' and 'The Personal Data Protection Factbook', both works edited by Thomson-Aranzadi. Alvaro further participates in frequent conferences, courses and forums as keynote speaker presenting on his areas of expertise.

Écija Bernal, Hugo

Hugo is managing partner at Ecija Abogados. He obtained his Doctorate in International Commercial Law and has completed postgraduate research and studies in International Law, European Union Law and Intellectual Property at the University of Oslo (Norway), South Western Community College (SWOCC) Coos Bay campus (Oregon, USA) and Skidmore College (New York, USA).

Hugo's national and international trajectory alongside in-depth experience in various sectors has brought him to advise leading national and multinational companies, public and private entities as well as assume sole legal advisor roles for community and international projects, various having been for the European Commission in projects on the European level, seeking expert legal advice regarding international matters.

He is a frequent contributor to national and international specialised press and magazines such as 'The John Marshall of Computer and Information Law'. Hugo has directed and authored various successful publications, including 'The Audiovisual White Book', 'The Entertainment Factbook 2003', and most recently 'The Media White Book 2005'.

Hugo is founder and director of the Masters in Audiovisual Law at the Instituto de Empresa, Madrid. He also is professor of Commercial Law and Intellectual Property at leading business schools throughout Spain such as Instituto de Empresa, ICADE, and other Spanish Universities. He further contributes to his expertise sectors by attending major business training forums and events in Spain as keynote speaker.

Gil Krokun, Jennifer

Jennifer obtained her law degree from the Complutense University in Madrid, with a Masters in IT Law. She holds a strong expertise in the problems and issues behind data protection for matters concerning Internet. Currently, Jennifer is Director of Consulting for the New Technologies and Data Protection practice areas in Ecija Abogados, leading Adecuation and Adaptation projects for both public and private clients. She has also collaborated as author for the successful publication 'The Personal Data Protection Factbook', edited by Thomson-Aranzadi. Jennifer further participates in frequent conferences, courses and forums as keynote speaker presenting on her areas of expertise.

Gómez-Skarmeta, Antonio F.

Antonio F. Gómez-Skarmeta received the M.S. degree in Computer Science from the University of Granada and B.S. (Hons.) and the Ph.D. degrees in Computer Science from the University of Murcia Spain. Since 1993 he is a Professor in the Deparment of Communications and

Information Engineering from the University of Murcia, Spain, and from 2001-2005 chair of the department. Additionally he has participated in several EU projects in different areas as collaborative working environment, security in IP networks and mobility and security in IPv6 where several advanced services like multicast, multihoming, security and adaptative multimedia applications are being deployed. His current research interests include security in mobile computing and networks, ad-hoc networks and distributed system. He has published more than 130 international papers in journals and conferences, being also member of several international program comitees.

Martínez, Gregorio

Gregorio Martínez received an MSc and PhD degree in Computer Engineering at the University of Murcia (Spain). In 1997 he started to work in the Computer Service of the same University on various projects related to security in communications. In 1999 he started as research staff in the Department of Information and Communications Engineering of the University of Murcia. In 2001, he was appointed lecturer in the same department.

His scientific activity is mainly devoted to security and the distributed management of IPv4/v6-based communications networks. He is working on different national and international research projects related to these topics, as the Euro6IX, SEINIT and POSITIF EU IST projects. He has published several papers in national and international conference proceedings and journals.

Palet Martínez, Jordi

Jordi Palet Martínez, Consulintel CEO/CTO, has been working in computers, networking and telecomm business during the last 20 years.

He has been involved in the IPv6 Forum, as chair of the Education & Awareness Working Group, since the Forum foundation and is member of the Technical Directorate. Jordi is also a member of the IPv6 Logo Committee, responsible for the 'IPv6 Ready' Program.

Jordi is frequent lecturer in several events and has given talks in different conferences across the world, as an expert mainly in IPv6 and related aspects (QoS, multicast, anycast, mobility, security, multihoming, ...) and his involvement in R&D projects.

He is frequently involved in ISOC, IETF, RIPE and other standardizations foras and related meetings. He also is working in the European Commission IPv6 Task Force, where he was one of the main contributors. He is co-author of numerous IETF documents.

Jordi is active member of non-profit organizations for the dissemination of technologies and telecommunications/Internet. He is an active member of the Spanish IPv6 Task Force, and the IPv6 Task Force Steering Committee. He is also cooperating in several European and worldwide IPv6 Task Forces and similar bodies.

Jordi is involvement in several R&D projects and was the designer of Euro6IX and indeed is the Scientific Project Coordinator. He is also heavily involved in other EC IST projects, including 6POWER (where is also the Scientific Coordinator), 6QM, Eurov6, IPv6 TF-SC, 6LINK and the IPv6 Cluster. He is also involved in several national R&D projects and the Eureka project PlaNetS.

Sáiz Peña, Carlos Alberto

Carlos obtained his law degree from the University of Alcala, and his Masters in Jurisprudence from the University Pontifica Comillas (ICADE) in Madrid. Carlos has advanced studies in Intellectual Property and New Technologies law. He is a partner at Ecija Abogados.

Currently, Carlos is the head of the New Technologies and Data Protection practice groups at Ecija, directing Consulting and Adecuation projects for leading businesses and multinational clients in their compliance with the data protection regulation. In addition, he is also highly involved in all of the firm's initiatives related with New Technologies.

Carlos has participated in various works as author, such as 'The Audiovisual White Book', and 'Internet: Contracts: Applications and Practical Suggestions', and 'The Personal Data Protection Factbook', all of which have been edited Thomson-Aranzadi. He is also a frequent keynote speaker at various seminary, courses and forums for his numerous expertise areas.

figures and links

Table of Figures

Links to IPv6

- Euro6IX http://www.euro6ix.org
- IETF http://www.ietf.org
- IPv6 Task Force http://www.ipv6tf.org


Euro6IX
IPv6:The New Internet

Introducción

- ¿En qué consiste el nuevo Protocolo de Internet IPv6? Principales aspectos y características
- El despliegue de IPv6: situación actual y experiencias
- Implicaciones y consecuencias de su despliegue
- Consecuencias legales:
  - ¿Cómo puede afectar IPv6 al derecho a la intimidad de los usuarios?
  - ¿Podría considerarse una dirección IP como un dato personal?
  - ¿Cómo podría IPv6 ayudar en la lucha contra la piratería?

- **¿A quién va dirigido este Manual?**

Abogados de empresa
Responsables de Seguridad
Abogados
Consultores
Directivos
Directores de Auditoría Interna
Directores Generales
Operadoras de Telecomunicaciones
ISP´s
Titulares de Páginas Web
Directores de Organización
Fabricantes de Tecnología

IPv6 Aspectos Legales

índice

índice

uno

dos

índice

índice

tres

índice

cuatro

Prólogo

El crecimiento extraordinario de las nuevas tecnologías y, en especial, la futura implementación del Protocolo IP en su versión 6 (IPv6) abre un enorme abanico de posibilidades, actividades y nuevas formas de comunicarse, trabajar, comprar, relacionarse con otras personas y, en definitiva, desempeñar las tareas cotidianas de nuestra vida.

Por ejemplo, la posibilidad de localizar el lugar exacto donde se encuentra un determinado dispositivo móvil, tener una nevera capaz de conectarse al supermercado y efectuar un pedido de los productos que faltan o poder decidir los destinatarios autorizados a recibir una canción obtenida a través de Internet, son ejemplos de situaciones donde IPv6 se convierte en un elemento casi esencial que permite, junto con otros factores, que estas actividades comiencen a ser una realidad.

En este sentido, IPv6 cobra especial relevancia en esta materia ya que la versión 4 del protocolo IP (IPv4), en la actualidad, cuenta con numerosas limitaciones que impiden un mejor desarrollo de estos nuevos avances y su eficaz funcionamiento. Algunas de estas limitaciones son, por ejemplo, que sus especificaciones técnicas no permiten fácilmente su extensión, el número de direcciones IP se encuentra limitado, etc.

Por eso, si bien estos nuevos avances basados en IPv6 tienen como principal objetivo mejorar la calidad de vida de sus usuarios, por otro lado, obligan, en primer lugar, a efectuar importantes labores de desarrollo e investigación tecnológica que requieren una importante implicación internacional y, en segundo lugar, tener en cuenta las implicaciones jurídicas que la implantación de IPv6 conlleva, a los efectos de asegurar que su uso quede dentro del ámbito legislativo aplicable y que, por lo tanto, su implementación no vulnere la legislación ni los derechos y libertades que les son reconocidos a los usuarios.

La alarma acerca de las implicaciones legales que IPv6 podría tener ya fue puesta de manifiesto por el Grupo del Artículo 29 a través de su Opinión 2/2002 relativa al uso de identificadores únicos: El ejemplo de IPv6, de 30 de mayo. En concreto, la principal preocupación se basaba en la existencia de "Identificadores Únicos" en determinados tipos de direcciones IPv6. Estos identificadores son capaces de dejar rastros a modo de "huella", por ejemplo, cada vez que una persona accede a una página web, lo cual permitirá que se obtenga un estudio detallado del perfil, gustos, etc, de esta persona y en definitiva, efectuar rastreos de la navegación de los usuarios.

Preguntas del tipo "¿qué consecuencias legales pueden existir?" o "¿se verá la intimidad de los usuarios afectada por IPv6?", "¿existen implicaciones en materia de protección de datos?", "¿qué está permitido hacer con la información que se tiene acerca de los hábitos de navegación de un usuario?", etc, comenzaron entonces a producirse y salir a la luz, exigiéndose, cada vez más, una respuesta clara a cada una de ellas.

Prólogo

Sin embargo, si bien estas dudas versaban sobre diferentes ámbitos, la principal preocupación se centró en las posibles vulneraciones que IPv6 podría conllevar con respecto al derecho a la intimidad o privacidad de sus usuarios, como es denominado este derecho en los países anglosajones.

Por otro lado, también surgieron dudas acerca de las consecuencias jurídicas que podrían existir, por ejemplo, tras la consideración de una dirección IP como un dato personal.

Por todo ello, pronto nacieron iniciativas que levemente comenzaban a apuntar estos temas jurídicos, ya que se tomó conciencia de que el buen desarrollo y acogida de IPv6 por sus futuros usuarios, estaba directamente relacionado con el grado de confianza que los mismos depositaran en dicho Protocolo. Para ello, los usuarios deberían conocer no sólo sus implicaciones técnicas (qué es; cómo funciona, qué ventajas tiene su uso; qué conlleva su utilización, etc) sino los aspectos jurídicos relacionados con el mismo (su legalidad; la posible vulneración de derechos; obligaciones de los proveedores, etc).

Dentro de las iniciativas que han ido surgiendo como consecuencia de las labores de investigación, diseño de arquitectura e implantación de IPv6, nació el Proyecto Euro6IX (Red Europea de Intercambiadores de Tráfico IPv6) cuya principal misión fue, por un lado, potenciar las labores de investigación sobre esta nueva versión y, por otro, facilitar su rápida implementación en Europa.

Asimismo, dentro del Proyecto Euro6IX, se entendió como un pilar fundamental del mismo, la necesidad de llevar a cabo un estudio jurídico de las implicaciones legales de este Protocolo, llevándose a cabo un profundo análisis en materia de intimidad, datos personales y protección de derechos de propiedad intelectual e industrial. En este sentido, parte de este libro recoge los estudios realizados sobre esta materia durante el desarrollo del mencionado Proyecto.

Por todo ello, a través de este libro, se pretende aportar una serie de conocimientos básicos de carácter técnico, necesarios para conocer qué es IPv6, su funcionamiento y el estado actual de su implementación a nivel mundial para, posteriormente, entrar a conocer los posibles problemas y soluciones, desde un punto de vista jurídico, que pudieran existir en los siguientes ámbitos:

- Derecho a la intimidad o privacidad
- Protección de datos personales
- Derechos de propiedad intelectual e industrial

Prólogo

Estas consideraciones jurídicas no sólo se observarán con relación a las actividades de desarrollo de infraestructuras, redes, etc, sino que dichas consideraciones se tendrán en cuenta en la regulación jurídica de los servicios que se prestan a través de dichas infraestructuras y redes, por ejemplo, servicios de VoIP, intercambio de ficheros, servicios de mensajería instantánea, acceso a contenidos audiovisuales, etc.

Una vez analizados los posibles problemas jurídicos derivados de IPv6, se expondrán a través de este libro posibles soluciones, las cuales pueden ser de diversa naturaleza: utilizar herramientas incorporadas a IPv6 como medio de protección; posibilidad de nuevos desarrollos normativos que regularicen dichos problemas o, en otras ocasiones, búsqueda de los modos más factibles de dar cumplimiento a las obligaciones legales de la forma más sencilla posible.

Por todo ello, el conocimiento del fenómeno IPv6, de su funcionamiento, sus ventajas, sus inconvenientes y las soluciones técnicas y jurídicas existentes para los mismos, constituye un paso obligado para potenciar su implantación exitosa, así como su conocimiento por parte de los usuarios futuros.

Así, IPv6 ya cuenta con el apoyo de importantes entidades que abogan por su implantación definitiva, por ejemplo, universidades, empresas tecnológicas, grandes empresas de telecomunicaciones así como, entre otras, importantes empresas dedicadas a la telefonía móvil que entienden que, dado que el número de teléfonos móviles supera en la actualidad al número de teléfonos fijos, IPv6 es la única arquitectura posible capaz de dar soporte a teléfonos móviles a través de los cuales es posible la conexión a Internet y a la correcta prestación de los servicios que vienen demandándose por los usuarios de este tipo de telefonía.

Además, en la actualidad la gran mayoría de proveedores de redes de investigación, públicas y comerciales, ya están funcionando con IPv6.

Todas estas iniciativas ponen de manifiesto que IPv6 cada vez está más lejos de continuar siendo un proyecto para irse configurando como una realidad que pretende afectar a todas las vertientes de la vida cotidiana, mejorando la capacidad de comunicación entre sus usuarios y dando paso a la Nueva Era de Internet.

Euro6IX
IPv6:The New Internet

1. El Protocolo IPv6

1.1. ¿Que es IPv6?

IPv6 es una actualización del Protocolo de Internet, el cual es clave para el funcionamiento de la Red. El Grupo de Trabajo de Ingeniería de Internet (Internet Enginnering Task Force, IETF), desarrolló las especificaciones básicas de IPv6 durante los años 90, tras una fase de diseño competitivo empleada para seleccionar la mejor solución global. La principal motivación para el diseño y desarrollo de IPv6 fue la necesidad de ampliar el número de direcciones disponibles en Internet, permitiendo así la intercomunicación de miles de millones de nuevos dispositivos (agendas electrónicas, teléfonos móviles, dispositivos, etc.) y nuevos usuarios (países como China, India, etc.). El uso de banda ancha para todos, y tecnologías "siempre conectadas", como xDSL, cable, ethernet hasta el hogar, fibra hasta el hogar, comulaciones a través de la red eléctrica (PLC), etc., son también factores determinantes para la demanda de IPv6.

Aún cuando el protocolo existente, IPv4, proporciona un espacio de direcciones de 32 bits, que teóricamente son 2^{32} direcciones globales únicas (aproximadamente 4.000 millones), en la práctica, el número de direcciones globales IPv4 que pueden ser utilizadas es bastante inferior, debido a las ineficiencias en la asignación y uso de las direcciones. IPv4 tiene una capacidad limitada inherente para permitir la expansión de Internet y por tanto no permite conectar miles de millones de dispositivos cuando sea apropiado. La traducción de direcciones de red (Network Address Translation, NAT), conjuntamente con direcciones IPv4 privadas, ha permitido la prolongación de la vida útil de IPv4. Sin embargo, NAT añade complejidad al despliegue de nuevos modelos extremo a extremo, inhibiendo el crecimiento de Internet y la innovación, incluyendo aquellos servicios como "siempre-conectado" y "peer-to-peer", que requieren acceso seguro y constante a dispositivos como por ejemplo en redes domésticas. IPv6 ha sido concebido para facilitar estos dos objetivos, proporcionando una capacidad de direccionamiento virtualmente ilimitada que puede direccional hasta 2^{128} dispositivos (hasta 340.282.366.920.938.463.463.374.607.431.768.211.456).

IPv6 juega un papel fundamental en el despliegue de redes celulares 3G, aplicado con nuevos servicios y aplicaciones multimedia, y su importancia fue reconocida por la Comisión y el Consejo Europeos, ya en el año 2002, conjuntamente con banda ancha y 3G. Consecuentemente, el plan de acción eEurope 2005 se centró en *"la amplia difusión de la disponibilidad y uso de redes de banda ancha a través de la Union en el 2005 y el desarrollo del protocolo de Internet IPv6 ... y la seguridad de las redes y la información, eGobierno, eEnseñanza, eSalud y eNegocios"*.

Cuestiones iniciales

Hoy, IPv6, 3G y banda ancha (incluyendo PLC), están comenzado a despegar, y un amplio abanico de servicios y aplicaciones pronto emergerán para dejar de ser un sueño. Estas tecnologías activan la visión de la Inteligencia Ambiental (Ambient Intelligence), con escenarios inteligentes, que podrían comenzar con hogares digitales activados con IPv6, *e*Seguridad en vehículos, y un mejor operación y administración de las redes que permitirán a los ISPs ofrecer todos estos servicios y sin duda, muchos más.

1.2. Principales diferencias entre IPv6 e IPv4

Como ya se ha indicado anteriormente, IPv6 fue originalmente diseñado con una razón de peso en mente: La necesidad de mas direcciones.

Por supuesto, hay soluciones alternativas, como NAT, que ya hemos mencionado, pero no funcionan tan fácilmente de forma que permitan el crecimiento, nuevos servicios y aplicaciones mejoradas, y en general la innovación. Además, estas técnicas hacen de Internet, las aplicaciones, e incluso los dispositivos algo mucho mas complejo, y esto supone también un incremento del coste, mientras que IPv6 puede hacer que, a medio/largo plazo, cada dispositivo IP sea más asequible, mas poderoso e incluso consuma menos energía (lo cual no es sólo importante para la conservación ecológica, sino también para permitir baterías de mayor duración en dispositivos portátiles como teléfonos celulares).

Usemos un sencillo ejemplo para entender, sin tecnicismos, que es NAT. Supongamos que dos personas que hablan el mismo lenguaje, digamos Castellano, necesitan usar un determinado medio de comunicación, que sin embargo no permite el uso de Castellano. Para permitir dicha conversación, por tanto, necesitan usar traductores situados junto a cada uno de los dos participantes en dicha conversación, a cada lado del canal de comunicación. Es obvio que algunos matices de la comunicación se podrían perder con las traducciones. Esto es muy similar a lo que hoy ocurre con Internet con IPv4: La falta de comunicaciones extremo a extremo impide que los servicios y aplicaciones tengan la capacidad de sacar todo el provecho de la red, haciéndolo todo mucho más complejo e incrementando los costes de administración.

También es cierto que NAT ha sido fundamental para permitir la penetración de Internet en nuestra vida diaria, debido a la falta del espacio de direcciones públicas IPv4 que era requerido para dicho crecimiento, mientras IPv6 no estaba lo suficientemente maduro. Pero hoy este ya no es el caso y NAT puede ser considerado como una especie de demonio para la innovación.

Consecuentemente, el diseño de IPv6 fue una forma oportunística de mejorar Internet, con nuevas ventajas, además de la capacidad para expandir el espacio de direcciones, tales como:

Cuestiones iniciales

- Auto-configuración y re-configuración sin servidores ("enchufar y funcionar", "plug and play"). Con esta característica Internet se simplifica, en el sentido de que es más fácil conectar automáticamente cualquier dispositivo a la red. No hay motivos para pedir a los usuarios que configuren nunca más los dispositivos, especialmente considerando que los nuevos dispositivos no serán "sencillos" ordenadores con teclado y pantalla, sino electrodomésticos, dispositivos de todo tipo, sensores, etc., los cuales no tienen este tipo de interfaces para poder ser configurados. En IPv4 esto no se puede realizar salvo que en la red se haya instalado un servidor (para el protocolo DHCP), lo que implica un coste superior para el propio servidor y su mantenimiento.

- Mecanismos de movilidad mas eficientes y robustos. IPv6 ha sido diseñado bajo la perspectiva de un nuevo mundo "nómada". Usuarios y dispositivos tienen a movilizarse mas que nunca. La conectividad es importante incluso cuando nos desplazamos, de tal forma que podamos utilizar servicios mejorados, especialmente en entornos sin cables. IPv4 también permite movilidad, pero es muy ineficiente comparada con la movilidad en IPv6.

- Seguridad extremo a extremo con autenticación y encriptación embebidas en la capa IP. IPsec es el protocolo de seguridad, el mismo que en el caso de IPv4. La principal diferencia es que IPv4 no obliga al soporte de IPsec, lo que implica que no siempre esta disponible. Además, en IPv4, debido al uso de NAT, a menudo no es posible utilizar IPsec extremo a extremo, salvo que se posean los conocimientos necesarios para configurar un túnel o VPN (Red Privada Virtual, Virtual Private Network), entre las dos estaciones que desean establecer dicha comunicación y se atraviesen los NAT. Este aspecto se describe con mas profundidad posteriormente en este mismo capítulo.

- Cabecera con una formato mejorado e identificación de flujos. Los diseñadores del protocolo IPv6 sacaron provecho de los conocimientos adquiridos con la experiencia por el uso de IPv4 durante los últimos años, de forma que pudiera mejorarse la forma en que los datos se codifican para formar la cabecera del protocolo IPv6 y consecuentemente mejorar la operación de la red. Al mismo tiempo que la cabecera ha sido simplificada, hemos agregado nuevas funcionalidades, siendo una de ellas la identificación de flujos, lo cual permitirá en un futuro próximo una mejor operación de los mecanismos de calidad de servicio (QoS) en Internet.

- Soporte mejorado de multidifusión. IPv6 incluye soporte mejorado de multidifusión (multicast), dado que se trata de una característica embebida en el protocolo, la cual es fundamental para el uso de redes de banda ancha para la distribución de contenidos.

- Extensibilidad: Soporte mejorado para opciones/extensiones. Por último, pero no menos importante, IPv6 ha sido diseñado teniendo en cuenta las posibilidades para su crecimiento. No deseamos repetir errores y llegar a la situación de descubrir, en unos pocos años, que del mismo modo que diseñamos IPv4 de tal forma que ha llegado a ser un impedimento para la extensión de Internet, pueda ocurrir con IPv6. La forma en que IPv6 trabaja permite incorporar nuevas características o piezas del protocolo (las que denominamos cabeceras de extensión), sin necesidad de actualizar todos los dispositivos de la red. Sólo aquellos dispositivos que precisen usar determinadas extensiones tienen que ser actualizados, del mismo modo que hoy todos los sistemas operativos y aplicaciones son frecuentemente actualizados, de una forma automática, transparente para el usuario.

1.3. La Transición a IPv6

Un aspecto muy importante desde que se inició el diseño de IPv6 fue el reconocimiento de que tendría que coexistir en la red con IPv4 durante un largo período de tiempo. Esto es debido al hecho de que ya existen millones de dispositivos, aplicaciones y servicios, los cuales no pueden ser desconectados ni tan siquiera por un momento. Internet ha llegado a ser una infraestructura crítica, y no hay modo alguno de pararla, ni tan siquiera por una única noche, realizar una actualización y tener IPv6 funcionando en toda la Red. Es también fácil entender que aún cuando fuéramos capaces de hacerlo así, todavía habría dispositivos que no podrían ser actualizados para soportar IPv6, por ejemplo en aquellos casos en los cuales el fabricante ha desaparecido y posiblemente no tenemos acceso al código existente en su interior para actualizarlo nosotros mismos.

Por este motivo, IPv6 ha sido diseñado junto a un conjunto de mecanismos de transición, los cuales permiten la coexistencia de ambos protocolos, IPv4 e IPv6, tanto tiempo como sea preciso, lo cual dependerá de innumerables factores, escenarios de red, sectores de negocio, etc. Además, estos mecanismos de transición facilitan la integración de IPv6 en la red Internet existente hoy con IPv4.

Técnicamente hablando, podemos decir que IPv6 esta maduro: Hoy es posible hacer con IPv6 todo lo que podemos hacer con IPv4 y mucho mas. Claramente podemos prever una mayor desarrollo de nuevos servicios y aplicaciones gracias a la implantación de IPv6. IPv6 traerá de nuevo la innovación a Internet, la innovación que el despliegue de NAT con IPv4 llego a detener.

Un par de años atrás, muchas redes tan sólo soportaban IPv6 y muy pocas IPv6. Hoy la situación ha cambiado radicalmente y más y más redes comerciales ya soportan IPv6. En un futuro próximo, veremos toda la red Internet soportando tanto IPv4 como IPv6, e incluso llegaremos al punto en que algunas redes dejarán de soportar IPv4. Por supuesto, la comu-

nicación extremo-a-extremo con IPv4 seguirá siento posible, porque utilizaremos mecanismos de transición, pero en sentido inverso al que lo hacemos ahora cuando deseamos utilizar IPv6 en redes que solo soportan IPv4.

Hemos de destacar además, que la gran mayoría de las redes de investigación y educación del mundo entero soportan IPv6 desde hace más de un año.

Diversas instituciones públicas y privadas están fuertemente vinculadas con el compromiso de impulsar el despliegue de IPv6, incluyendo la Comisión Europea, el Departamento de Defensa Norteamericano, etc.

Para más información acerca del estado del despliegue y el soporte global hacia IPv6, refiérase a las publicaciones del IPv6 Cluster "Moviéndose a IPv6 en Europa"(1) ("Moving to IPv6 in Europe") e "IPv6 y banda ancha"(2) ("IPv6 and Broadband").

El "The IPv6 Portal"(3) también ofrece información actualizada acerca de la situación del despliegue en todo el mundo.

1.4. Actividades Europeas de I+D al respeto de IPv6

El programa de Tecnologías de la Sociedad de la Información de la Comisión Europea ha financiado gran número de proyectos con un importante enfoque al respecto de actividades de Investigación y Desarrollo de IPv6. Estos proyectos han representado una inmensa inversión en nombre de la CE (cerca de 90 Millones de Euros) y los participantes en dichos proyectos.

Estos proyectos pueden clasificarse en dos grupos. Los proyectos del primer grupo, que podemos denominar "Proyectos de IPv6", han tenido un énfasis específico en IPv6, siendo su principal objetivo la investigación y desarrollo del protocolo mismo. Los proyectos del segundo grupo, que podríamos denominar "Proyectos relacionados con IPv6", utilizan IPv6 como parte de unos objetivos mucho más amplios.

Los proyectos han estudiado un amplio abanico de áreas complementarias y aspectos técnicos relacionados con IPv6 (por ejemplo: transición de IPv4 a IPv6, Calidad de Servicio, etc.). Dos grandes plataformas de experimentación han investigado el despliegue real de IPv6, siendo Euro6IX una de ellas. Otros proyectos se han dedicado a la promoción de IPv6, e incluso ha habido proyectos específicos para dirigirse a la dimensión política.

Además, todos los proyectos de uno u otro modo relacionados con IPv6, han colaborado en el marco del IPv6 Cluster desde Junio de 2001, y un proyecto específico, 6LINK, soportó las actividades de dicho Cluster.

(1) http://www.ipv6tf.org/news/newsroom.php?id=169 | (2) http://www.ipv6tf.org/news/newsroom.php?id=988 | (3) http://www.ipv6tf.org

Cuestiones iniciales

2. El Proyecto Euro6IX (Red Europea de Intercambiadores de Tráfico IPv6)

2.1. ¿Que es el proyecto Euro6IX?

Euro6IX ha sido el mayor proyecto, de su ámbito, hasta ahora financiado por el programa europeo IST. Su finalidad fue el soporte de la rápida introducción de IPv6 en Europa. Para la consecución de esta meta, el proyecto definió un plan de trabajo con todos los pasos necesarios incluyendo: el diseño de la red Pan-Europea (con IPv6 nativo) y su implantación; la investigación de los servicios avanzados de dicha red; el desarrollo de aplicaciones que fueron validadas mediante la vinculación de grupos de usuarios y pruebas internacionales; y actividades de divulgación activa, incluyendo eventos y conferencias, contribuciones a estándares (IETF, RIPE y otros), publicación de informes, y promoción de todos los resultados del proyecto a través de la web del mismo.

Euro6IX, comenzó en Enero de 2002, construyendo redes IPv6 nativas y dedicadas, involucrando operadores, ISPs y redes de investigación y educación, en una aproximación complementaria y considerando otros aspectos como aplicaciones, Intercambiadores de Tráfico y aspectos legales.

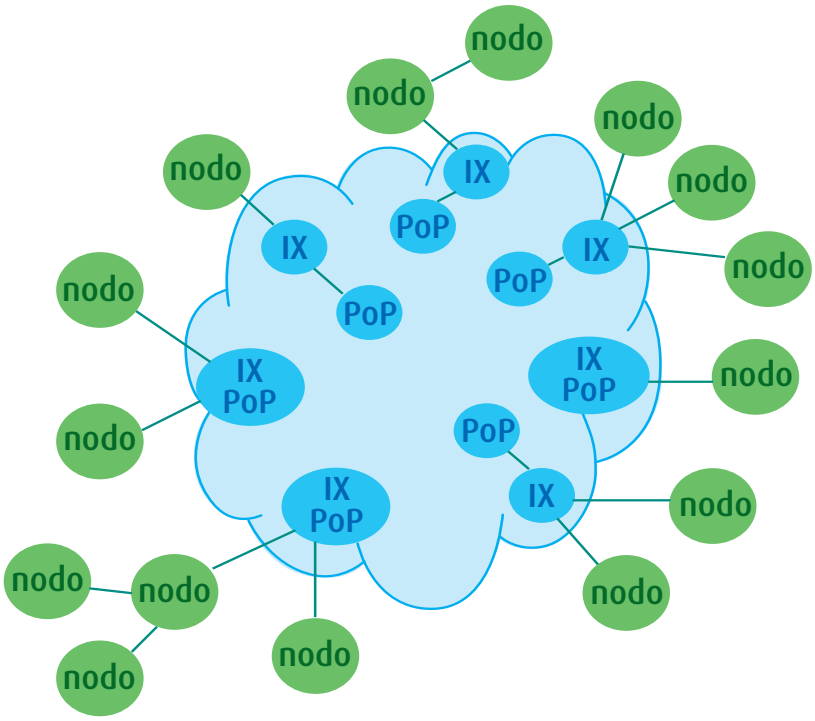
El proyecto ha investigado, diseñado y desplegado una red IPv6 nativa Pan-Europea, denominada red de pruebas Euro6IX. Ha incluído los servicios más avanzados obtenibles de la tecnología actual, y ha seguido la arquitectura de la actual Internet (basada en IPv4), considerando todos los niveles precisos para la implantación mundial de IPv6, la nueva generación de Internet. La infraestructura de Euro6IX ha aunado diversos niveles de red:

- **IX:** Intercambiadores regionales de tráfico IPv6 nativo.
- **Troncal:** Red troncal Pan-Europea que interconecta los Intercambiadores Regionales y crea el nivel superior en la jerarquía de la red.
- **Nodos:** Proveedores de Servicios, ISP's y otros tipos de proveedores, accediendo al troncal de la red, para proporcionar servicios IPv6 y acceso a los usuarios. Los usuarios serán conectados a través de una gran variedad de tecnologías de acceso, incluyendo redes heredadas IPv4 y otros servicios, cuando no se pueda disponer de enlaces nativos IPv6.

Este nivel incluye un conjunto de usuarios académicos, de investigación y no-comerciales, generando tráfico IPv6 nativo.

El siguiente esquema muestra la abstracción de estos niveles de la red.

Cuestiones iniciales



Esquema abstracto de la red de pruebas de Euro6IX

Euro6IX ha ofrecido servicios avanzados de red y un repositorio de aplicaciones con soporte nativo de IPv6, las cuales han sido portadas, adaptadas o mejoradas y puestas a disposición para la realización de pruebas incluso a actores externos al proyecto.

El tráfico nativo IPv6 ha sido resultante tanto de estas aplicaciones específicas, como de otras genéricas, funcionando con IPv6 (por ejemplo navegadores web).

La validación ha sido realizada en un contexto realista donde los diferentes actores y roles, que en la actualidad existen en Internet, se han extrapolado a la nueva generación basada en IPv6. Esta validación se ha realizado a través de la vinculación de grupos de usuarios existentes y otros creados por el propio proyecto, tanto por medio de pruebas internas como públicas y otros eventos.

Además, se realizaron innumerables actividades de divulgación, promoción, relaciones públicas, y coordinación, en clusters, organizaciones de estandarización y terceras partes interesadas, con el objetivo de facilitar la máxima visibilidad de los resultados del proyecto y obtener el mayor impacto posible.

Cuestiones iniciales

El éxito del proyecto Euro6IX se ha medido frente al nivel de alcance de:

- La provisión de una conectividad eficiente y servicios avanzados de red, para la red IPv6 Europea.
- Vinculación de entidades de desarrollo y grupos de usuarios no-comerciales (beta-testers), para validad dicha red, los servicios avanzados y las aplicaciones.
- Promoción del interés hacia IPv6 por parte de usuarios e ISP's, entidades de normalización y otros proyectos relacionados.

2.2. Objetivos Perseguidos

El **principal** objetivo del proyecto Euro6IX ha sido la investigación de la arquitectura apropiada, el diseño y la implantación de la primera red Pan-Europea, no comercial, de Intercambiadores de Trafico Internet IPv6. Ha conectado diversos puntos Intercambiadores regionales de tráfico IPv6, a través de Europa, y alcanzará el mismo nivel de robustez y calidad de servicio que actualmente ofrecen redes similares IPv4. Esto es:

- Investigar y diseñar una red nativa IPv6, que sigue la arquitectura jerárquica existente en la Internet global, incluyendo:
  1. Un conjunto de Intercambiadores regionales nativos IPv6;
  2. Una red troncal que conecta los intercambiadores;
  3. Un nivel secundario de acceso, nodos, para usuarios, corporaciones, sitios e ISP's.
- Implantar la red nativa IPv6, siguiendo dicha arquitectura.
- Probar, ajustar y mejorar los principales protocolos, algoritmos y técnicas necesarias para implantar la red y los servicios avanzados.

Los mayores suministradores Europeos de Telecomunicaciones (incumbentes), han formado parte del proyecto. Ello permitió cubrir las áreas geográficas de mayor crecimiento en cuanto al número de usuarios, y refleja la importancia estratégica de este proyecto, para la introducción de IPv6 en Europa.

Como **segundo** objetivo, la red fue la base para la realización de actividades de investigación relacionadas con diversos aspectos de IPv6 como:

Investigación de la madurez de los servicios avanzados de red, así como la posibilidad de su introducción en la red Euro6IX, como son QoS/CoS, Movilidad IP, Anycast y multicast, seguridad, multihoming, renumeración, y lenguajes de políticas.

El desarrollo, porte, adaptación o mejora de aplicaciones preparadas para IPv6, las cuales se han liberado para su uso en las pruebas y por terceras partes ajenas al proyecto.

La investigación de las implicaciones legales del proyecto relacionadas con el direccionamiento de usuarios, red, y proveedores de servicios, y más concretamente Derechos de Propiedad Intelectual, protección de datos personales, y aspectos de privacidad relativos al direccionamiento en IPv6.

Como tercer objetivo, la red construida por Euro6IX se abrió al uso por parte de Grupos de Usuarios (existentes o creados por el propio proyecto), que se conectaron a la misma por medio de diversas tecnologías de acceso – móviles, xDSL, cable – e internetworking con redes heredadas IPv4, así como otros servicios, para probar las prestaciones de las futuras redes IPv6, y el uso no comercial nativo de los servicios y aplicaciones avanzadas IPv6. La Política de Uso Aceptable de la red excluyó la posibilidad de tráfico comercial.

La red fue ejercitada por los Grupos de Usuarios para validad y verificar el uso, características, y potencial, de la Internet de Siguiente Generación, en eventos de alta visibilidad y pruebas (tanto internas como públicas).

El cuarto objetivo ha sido la divulgación, relaciones públicas, promoción y coordinación con clusters, grupos relacionados, organizaciones de normalización (como IETF) y terceras partes, no vinculadas con el proyecto, y muy especialmente con proyectos similares como GEANT, 6WINIT, LONG, MIND, 6NET y cualesquiera que hayan estado disponibles a lo largo de la vida de Euro6IX.

2.3. Principales Actividades Desarrolladas

Euro6IX ha trabajado en muchos aspectos científicos relacionados con IPv6, involucrando un alto nivel de innovación. Podemos enumerar algunas de las principales actividades:

1. Pruebas de interoperabilidad y prestaciones.
2. Despliegue de movilidad IPv6 en redes de ISPs.
3. Agregación y delegación de direcciones en redes de ISPs e IXs.
4. Aspectos avanzados de encaminado en IXs.
5. Despliegue de IPv6 en redes de banda ancha.
6. Despliegue de multidifusión IPv6.
7. Despliegue de Calidad de Servicio en banda ancha.
8. Evaluación de mecanismos de autenticación, autorización y contabilidad con IPv6.

9. Despliegue de mecanismos de transición.
10. Despliegue de VPNs IPv6.
11. Gestión de redes basada en políticas con IPv6.
12. Seguridad distribuida con IPv6.

Podemos concluir afirmando que Euro6IX ha sido clave para la construcción de redes IPv6 a escala real, las cuales han proporcionado la experiencia requerida para facilitar el siguiente paso: La integración de IPv6 en redes comerciales, permitiendo así la provisión de nuevas oportunidades de negocio para ISPs en el camino hacia una nueva generación de servicios y aplicaciones que restablezcan la innovación en Internet.

2.4. Participantes del Proyecto

El proyecto Euro6IX ha involucrado la cooperación de los siguientes participantes:

- Telefónica I+D
- Consulintel
- Telecom Italia Lab
- Universidad Politécnica de Madrid
- Telscom
- Universidad de Southampton
- 6WIND
- Vodafone
- T-Systems
- BTexact Technologies
- Ecija & Asociados
- Ericsson Telebit
- Eurocontrol
- France Telecom RD
- novaGnet systems
- PT Inovação
- Universidad de Murcia

Información más completa de los participantes se haya disponible en http://www.euro6ix.org/partners/e_partners.php

Además, dos patrocinadores han participado también en el proyecto:

- Hitachi
- Swisscom Innovations

Más información acerca de los patrocinadores disponible en http://www.euro6ix.org/sponsors/e_sponsors.php

3. Seguridad en Redes IPv6: Introducción, Estado del Arte y Nuevos Retos

3.1. Introducción

El continuo crecimiento de Internet está obligando a que su arquitectura global evolucione para adaptarse a las nuevas tecnologías, sobre todo a aquellas que puedan dar soporte al creciente número de usuarios, dispositivos, servicios y aplicaciones. En este sentido, el protocolo IPv6 ha sido diseñado como el protocolo de nivel de red capaz de acomodar estos requerimientos.

La seguridad ha sido siempre mencionada como una de los servicios de valor añadido de mayor interés introducido por IPv6, al menos en teoría. De hecho, el desarrollo de redes de comunicaciones basadas en IPv6 presenta nuevos retos que necesitan ser abordados tanto en los laboratorios de investigación, como en las redes IPv6 operacionales; como ejemplo de estas última tenemos la que se ha diseñado y puesto en marcha como parte del proyecto europeo Euro6IX (acrónimo en inglés de *European IPv6 Internet Exchanges Backbone*) donde la mayor parte del trabajo de análisis y de investigación que aquí se presenta se ha llevado a cabo.

En el momento de hablar de seguridad en los sistemas de comunicaciones IPv6, la principal tecnología que debe ser mencionada es *IPsec*. De hecho, éste es el protocolo que ha sido diseñado y propuesto por el IETF, y aceptado por la comunidad internacional, como el estándar de facto para aportar seguridad a las redes IP (tanto IPv4 como IPv6). El hecho de estar en el nivel de red le hace ser una buena solución por varias razones; entre ellas las más significativas son:

- Permite bloquear la mayoría de los ataques tradicionales de bajo nivel tales como, por ejemplo, la utilización malintencionada de direcciones IP (conocido por el término en inglés de *IP address spoofing*) o la escucha de datagramas IP (*packet sniffing*). Esto representa un paso importante hacia la provisión de seguridad en redes IP, ya que estos ataques son normalmente muy fáciles de implementar y al mismo tiempo suelen ser muy efectivos cuando se llevan a cabo contra redes que no están protegidas con unas mínimas características de seguridad.

- Aporta un conjunto de mecanismos básicos de seguridad que están disponibles para los servicios y aplicaciones de más alto nivel. Esto permite solventar algunos de los problemas actuales que ocurren cuando diferentes servicios y aplicaciones definen e implementan sus propias medidas de seguridad que normalmente no son interoperables entre ellas y requieren un cierto nivel de intervención (y destreza en términos de seguridad) por parte de los usuarios. En este sentido, IPsec evita la duplicación de los servicios básicos de seguridad, tales como el control de acceso y la provisión de confidencialidad a un canal de comunicaciones concreto. Sin embargo, es importante mencionar que dado que IPsec está situado en el nivel de red, no es una solución completa cuando los servicios y aplicaciones a ser protegidos están más orientados a los usuarios que a la propia red; ejemplos de este tipo de servicios y aplicaciones son el correo electrónico y las aplicaciones de comercio electrónico tradicional o móvil.

En este sentido, destacar que IPsec añade chequeo de integridad, autenticación, cifrado y protección contra reenvío a las comunicaciones IP. Estas propiedades se utilizan para aportar seguridad *extremo-a-extremo* y también para establecer *túneles seguros* entre routers IP. IPsec también ha sido diseñado para aportar interoperabilidad y no afecta a las redes y dispositivos que no lo implementan. Resaltar también que IPsec es independiente de los algoritmos criptográficos actuales, y es capaz de adaptarse a nuevos algoritmos según éstos vayan siendo definidos y puestos en marcha.

Las características de seguridad de IPsec se basan en la utilización de dos componentes principales, a saber la cabecera AH (*Authentication Header*) y la cabecera ESP (*Encrypted Security Payload*). La primera de ellas, la cabecera AH, se utiliza para aportar integridad, autenticación y opcionalmente protección de reenvío a los datagramas IP, mientras que la cabecera ESP se utiliza para aportar los servicios que se acaban de indicar y adicionalmente cifrado de las comunicaciones.

Ambas cabeceras se pueden utilizar de diferentes maneras para proteger las comunicaciones IP, siendo las *redes privadas virtuales* (VPNs o *Virtual Private Networks*) uno de los escenarios más representativos y de los que mayor uso se hace. La principal motivación existente en relación con las VPNs es el hecho de que Internet se ha convertido en una infraestructura de comunicaciones popular y de bajo coste, lo cual está haciendo que las compañías consideren el extender sus propias redes privadas a través de Internet para comunicar diferentes sucursales o establecer canales de comunicación seguros con sus proveedores o clientes.

3.2. IPsec e IPv6

Tal y como se ha comentado antes, IPsec y sus dos cabeceras asociadas (AH y ESP) se pueden utilizar tanto con IPv4 como con IPv6. Dada esta afirmación, la siguiente cuestión que se debe de resolver es ¿qué tiene IPsec que esté directamente relacionado con IPv6? Varias son las respuestas a esta pregunta, aunque las que se pueden destacar como más representativas son:

- El diseño de IPsec se realizó como parte del desarrollo del nuevo protocolo IPv6; de hecho, si echamos un vistazo a como funcionaban los sistemas de comunicaciones en la década de los 90, éstos se basaban en el hecho de que los entornos de comunicaciones eran *amigables* y sin la existencia de elementos maliciosos; sin embargo, ésta es una hipótesis que dejó de ser válida hace unos años, cuando estas redes empezaron a ser usadas con un carácter mucho más comercial. Como tal, IPsec funciona tanto con IPv4 como con IPv6, pero ha sido definido como un componente de obligada implementación en las pilas que hagan uso del protocolo IPv6.

- Las características de seguridad ofrecidas por IPv6 han sido definidas para ser una parte integral de los servicios ofrecidos por IPv6 tales como la provisión de calidad de servicio o de movilidad, aunque esto es el teoría, ya que la realidad nos muestra que la integración entre estos diferentes servicios de red está aún lejos de ser efectivo, y mucha más investigación es necesaria tanto en las fases de diseño como de implementación. Como ejemplo de esta afirmación indicar que la gestión segura de dispositivos móviles en redes IPv6 representa en la actualidad un tema de investigación muy interesante que se encuentra aún en la fase de identificar escenarios y proveer soluciones parciales para cada uno de ellos.

- La flexibilidad del esquema de direccionamiento de IPv6 provee soporte de direccionamiento global para cualquier dispositivo, lo cual seguramente reducirá el uso de dispositivos NAT (acrónimo en inglés de *Network Address Translation*) debido a que las direcciones globales estarán ampliamente disponibles. En este sentido, IPv6 permite establecer de forma global comunicaciones extremo-a-extremo, posibilidad que no siempre está disponible en aquellas redes IPv4 que hagan uso de NAT y de tecnologías similares que permitan la conversión o la reserva temporal de direcciones IP. Esta funcionalidad es considerada como de gran relevancia para los servicios de red y aplicaciones de nueva generación con significativos requerimientos de seguridad, como es el caso de dispositivos móviles, sistemas de telefonía integral, vehículos que ofrecen servicios de conexión a Internet, dispositivos conectados a un red doméstica, etc.

- Las características de seguridad han sido diseñadas en IPv6 como cabeceras de extensión de manera que pueden ser fácilmente desactivadas cuando los aspectos de seguridad no son relevantes o el rendimiento de la red es de gran importancia, como es el caso de ciertos escenarios de movilidad donde hay un ancho de banda reducido o aquellos que se encuentran basados en pequeños dispositivos con ciertas limitaciones de computación o de batería, como puede ser el caso de las redes de sensores, por ejemplo.
- IPsec puede proveer protección directa a otros protocolos relacionados con IPv6, como es el caso de ICMPv6 (acrónimo en inglés de *Internet Control Message Protocol for IPv6*).

3.3. Aspectos a considerar cuando se activa la seguridad en redes IPv6

Las características que se acaban de mencionar aportan varias ventajas de interés a los sistemas de comunicaciones. Sin embargo, existen varios aspectos que deberían ser considerados, especialmente por parte de los diseñadores de red, antes de activar la seguridad en sus redes IPv6 ya sean éstas nativas o dual-stack IPv4/IPv6. El principal motivo para afirmar esto es que ciertas condiciones de las redes actuales dejan de ser válidas, sobre todo la hipótesis de que existe una *topología de red estática*, el considerar que hay un número determinado de puntos de acceso a la red que están *bajo control de los administradores* (que normalmente se implementan mediante cortafuegos) y que el tráfico estará principalmente en claro y sólo estará cifrado para servicios o aplicaciones muy concretos.

De hecho, activar la seguridad en redes IPv6 significa permitir autenticación y cifrado de comunicaciones *extremo-a-extremo* entre diferentes dispositivos y por lo tanto limitar de forma significativa la capacidad de los diferentes sistemas que implementan y controlan las políticas de seguridad o que realizan actividades de monitorización en pro de la seguridad de la red, tales como los cortafuegos o los sistemas IDS (del inglés *Intrusion Detection System*). Estas tareas pueden ser mucho más complicadas todavía si cabe, al tratar al mismo tiempo con la seguridad de dispositivos móviles IPv6, ya que la topología de la red puede cambiar con el tiempo, haciendo que las direcciones de los dispositivos y el encaminamiento sean (re)asignados dinámicamente con el tiempo.

Este hecho tiene una importante implicación sobre el modo tradicional de definir la seguridad en las redes, proceso que normalmente se encuentra basado en una primera fase de diseño que intenta identificar los límites de un sistema de información y las políticas de seguridad que deberían de ser aplicadas, normalmente en los dispositivos de seguridad localizados en los *puntos de acceso* a la red. En esta fase, la cual está normalmente relacionada con la aplicación de medidas de seguridad a nivel de red y de transporte en los

cortafuegos, los dispositivos finales y los usuarios no son normalmente considerados de forma prioritaria. De hecho, estos últimos son normalmente considerados en una fase posterior mediante la definición de las medidas de seguridad a nivel de aplicación de se deben de tomar, tales como el software antivirus que debe de ser usado o la política de actualización de software que se debe de aplicar.

Sin embargo, en las redes IPv6 estas circunstancias cambiarán con toda probabilidad para tener en cuenta la aplicación de medidas y políticas de seguridad también en los dispositivos finales, y todo ello como parte de una estrategia de seguridad completa. Este cambio de filosofía estará en directa sintonía con nuevos procesos de gestión distribuida de la seguridad dentro de los diferentes dominios administrativos.

Por otra parte, los diseñadores de seguridad también deberán tener en cuenta la dinamicidad de la topología, la cual es considerada en la actualidad como el contexto básico para definir y evaluar los riesgos y vulnerabilidades de la red y las alarmas relacionadas con los procesos de detección de intrusiones.

Además, el concepto de cortafuegos tendrá que ser actualizado desde su rol actual de dispositivo capaz de implementar filtrado, NAT, proxies y traducción de puertos para una topología de red concreta y normalmente con carácter estático, a un nuevo tipo dispositivo (o un conjunto de ellos) capaces de tratar con el dinamismo asociado con los nuevos esquemas de asignación de direcciones o de enrutado, con el cifrado de la parte de datos de los datagramas IP o con la existencia de esquemas no predecibles para asociar una dirección IP fuente o destino con un determinado usuario. De manera adicional, los sistemas de IDS necesitarán actualizar su definición actual de firmas asociadas con ataques a los nuevos que puedan aparecer con IPv6 y adaptarse, cuando ello sea posible, al direccionamiento dinámico y a una visibilidad limitada del contenido de los paquetes de datos que circulan por la red.

IPv6 y el derecho a la intimidad

1. Introducción

El buen desarrollo de IPv6 depende en gran medida de que los usuarios tengan confianza en dicho Protocolo y conozcan sus ventajas: autoconfiguración, más direcciones IP, movilidad optimizada, extensibilidad, posibilidad de mejora de calidad y seguridad, entre otras.

Por ello, si IPv6 comienza a generar dudas acerca del peligro que supondría la posibilidad de realizar un seguimiento de la navegación de los sus usuarios y la consecuente vulneración de su intimidad, la propagación de noticias sobre este tema a través de cualquier medio, podría perjudicar gravemente el desarrollo de este Protocolo.

De hecho, ya en los últimos años de la década de los 90, comenzaron a aparecer los primeros titulares acerca de las consecuencias que IPv6 tendría en temas de privacidad, como consecuencia del uso de "Identificadores únicos" en las direcciones IP configuradas en base a IPv6. En concreto, la preocupación entonces se basaba en la posibilidad de monitorizar a los individuos mediante el seguimiento de las actividades realizadas por Internet o contenidas en cada paquete de información transmitida.

Este debate cruzó el Atlántico y tanto el Consejo de Europa como el Grupo del Artículo 29 de la Comisión Europea reconocieron que es necesario tener en cuenta los aspectos relativos al derecho a la intimidad y privacidad en el desarrollo e implantación de IPv6. El objeto de este capítulo es analizar estas consideraciones, cómo éstas se encuentran o no reguladas por la actual normativa europea, si estas consideraciones se encuentran justificadas y, en su caso, qué pasos se deben llevar a cabo.

2. IPv6 y Privacidad

IPv6 ha sido llamado el Nuevo Internet o el Internet de la Nueva Generación. El principal problema que ha tenido la anterior versión del protocolo IP ha sido que Internet ha crecido tan rápido a lo largo de los últimos años que se preveía el próximo agotamiento de las direcciones IP existentes.

Las comunicaciones a través de Internet son posibles gracias a un sistema denominado IP (Internet Protocol) el cual requiere que cada ordenador, dispositivo o nodo conectado a la Red tenga una dirección, denominada dirección IP. La actual versión de este Protocolo de Internet es IP en versión 4 (IPv4), la cual se ha venido usando durante los últimos 20 años.

Adicionalmente, la distribución de direcciones IP en IPv4 estaba descompensada ya que un tercio del número de direcciones a distribuir a nivel mundial estaban reservadas, inicialmente, para Estados Unidos, de hecho, dos universidades estadounidenses disponían de más direcciones IP que la propia China.

2

IPv6 y el derecho a la intimidad

Ya los informáticos que crearon Internet vislumbraron este problema de insuficiencia de direcciones IP con IPv4 y comenzaron a desarrollar una versión básica de lo que hoy es IPv6. Esta nueva versión tiene la capacidad suficiente como para facilitar mil millones de direcciones IP por cada metro cuadrado de la Tierra. En términos matemáticos, este hecho se ha conseguido cambiando de una dirección IP de 32 bits con IPv4 a otra de 128 bits con IPv6, lo cual supone claramente un importante desarrollo de Internet y de las tecnologías con él relacionadas.

La transición de IPv4 a IPv6 es un paso enorme que necesita una importante inversión tanto en investigación y desarrollo como en tecnología, lo cual implica que finalmente estas actividades tengan una gran presencia y requieran una importante colaboración a nivel internacional.

Aparte del problema de falta de direcciones IP ya solucionado con IPv6, el desarrollo de IPv6 permitirá disponer de una arquitectura y diseño de Internet que potenciará servicios más rápidos, eficaces, de mejor calidad y más seguros. IPv6 resuelve ciertos asuntos existentes en el Internet actual y permite otros relativos a la conectividad extremo a extremo, autoconfiguración, seguridad embebida, movilidad, multidifusión y permite la transmisión de paquetes de información más grandes.

Si bien, la introducción de este nuevo protocolo de Internet es cada vez más necesaria e inevitable, continúa aumentando la necesidad de analizar los riesgos que para la privacidad podrían existir como consecuencia del diseño de direcciones IP basadas en Identificadores Únicos.

2.1. ¿Qué se entiende por Privacidad/Intimidad?

La privacidad o intimidad en el mundo europeo es de los principales derechos que corresponden a las personas, pero a su vez es uno de los más difíciles de proteger. Sin el derecho a la intimidad, otros derechos como el derecho a la libertad de expresión o de reunión tendrían mucho menos significado.

El respeto a la intimidad es importante por muchos aspectos. Por un lado, está relacionada con la parte de la vida de una persona que ésta permite que sea conocida por otros y, por otra parte, es la posibilidad de mantener ciertas parcelas de la vida propia de forma anónima.

La intimidad hace referencia a la posibilidad de controlar la información que un individuo decide compartir con otras personas. Por ejemplo, una persona puede decidir compartir su dirección con la tienda online en la que está comprando un libro pero, probablemente, no quiera que su dirección aparezca publicada en la página web y sea accesible para todos los visitantes de la misma, ya que en estos casos se estaría produciendo una vulneración de la intimidad de esta persona.

IPv6 y el derecho a la intimidad

En líneas generales, cuando se habla del derecho a la privacidad o a la intimidad, se hace referencia al derecho a:

- Mantener información personal para si mismo
- Tener la posibilidad de mantenerse anónimo o no identificado respecto a ciertas actividades personales o públicas. Estas actividades pueden incluir el derecho a ejercer libremente la libertad de reunión o actividades privadas como los hábitos de consumo o la manera de trabajar de alguien.
- Vivir cada uno su propia vida sin sentirse controlado por otros.
- Mantener comunicaciones privadas.
- Disponer de privacidad física y espacio propio.
- Tener la facultad de ser "dejados en paz", tanto como consumidores como ciudadanos.

En este sentido, parece que la única manera segura para evitar la vulneración del derecho a la intimidad es dejar de interactuar con el mundo que nos rodea. Lógicamente, esto, aparte de ser imposible, no es deseable para ningún ciudadano, por lo que se convierte en una necesidad de primer orden establecer cautelas para proteger la privacidad de las personas cuando se produzca esta interacción.

2.2. ¿Cuál es el fundamento del derecho a la intimidad?

A los efectos de definir las bases bajo las cuales se fundamenta el derecho a la intimidad es necesario tener en cuenta la Convención Europea para los Derechos Humanos y Libertades Fundamentales de la Persona de 1950.

Esta Convención, creada por el Consejo de Europa y abierta para ser ratificada por cualquier país europeo, pretendió potenciar la protección de los derechos humanos y las libertades fundamentales tras la Segunda Guerra Mundial. Asimismo, en esta Convención, se reconocen otros derechos tales como el derecho a la vida; derecho a un juicio justo; derecho contra la tortura, etc.

La definición del derecho a la intimidad contenida en el artículo 8 de la Convención se extiende a cuatro áreas donde el individuo tiene derecho a que su intimidad sea respetada:

- Vida privada
- Vida familiar
- Domicilio
- Secreto de las comunicaciones

Esta Convención fue adoptada con carácter previo a la creación de la Unión Europea (tal y como la conocemos actualmente). Sin embargo, puesto que los derechos humanos son

uno de los principales fundamentos de la Unión Europea y una de las condiciones principales para su legitimidad, los Jefes de Estado o Gobierno decidieron en el Consejo Europeo de Colonia (junio 1999) que era necesario formalizar estos derechos y asegurar su prevalencia en la Unión Europea. Esto condujo a la proclamación de la Carta de los Derechos Fundamentales de la Unión Europea, el 8 de diciembre de 2000.

El derecho a la intimidad recogido en la Convención de 1950 fue prácticamente trasladado al artículo 7 de la Carta, en el cual se establece:

"Toda persona tiene derecho a que se respete su vida privada y familiar, su domicilio y el secreto de sus comunicaciones".

2.3. ¿Cuál es la relación existente entre intimidad y protección de datos?

Desde la promulgación de la Convención de 1950, una nueva faceta de la intimidad comenzaba a desarrollarse, directamente vinculada con los avances tecnológicos que estaban ocurriendo y, en concreto, con el importante aumento de tratamientos automatizados de información. Esta nueva faceta de la intimidad vino a denominarse "protección de datos", convirtiéndose este concepto en el arma para proteger la intimidad frente a la nueva Era tecnológica.

En este sentido, si bien la Carta de los Derechos Fundamentales recogía el derecho a la intimidad ya contemplado en la Convención de 1950, introducía un concepto novedoso: el derecho a la protección de datos. Su artículo 8 establece lo siguiente:

1.- "Toda persona tiene derecho a la protección de los datos de carácter personal que la conciernan.

2.- Estos datos se tratarán de modo leal, para fines determinados y sobre la base del consentimiento de la persona afectada o en virtud de otro fundamento legítimo previsto por la ley. Toda persona tiene derecho a acceder a los datos recogidos que la conciernan y a su rectificación.

3.- El respeto de estas normas quedará sujeto al control de una autoridad independiente".

En este sentido, basta con apuntar que la implantación de IPv6 conlleva asimismo implicaciones en materia de protección de datos, algunas de las cuales serán tratadas brevemente en el presente Capítulo. No obstante, la principal problemática existente sobre este tema será abordada con mayor detenimiento en el Capítulo III de este libro.

2.4. ¿Qué reglas regulan la protección de datos?

Si bien, esta normativa será analizada con más profundidad en el apartado 3 del siguiente Capítulo, es conveniente adelantar que la primera legislación en materia de protección

IPv6 y el derecho a la intimidad

de datos puede remontarse a la Ley aprobada por el Estado de Hesse en Alemania en el año 1970. Posteriormente, se promulgaron otras legislaciones tales como la de Suecia (1973), los Estados Unidos (1974), Alemania (1977) y Francia (1978).

La primera legislación importante en esta materia a nivel europeo fue el Convenio del Consejo de Europa de protección de las personas con respecto al tratamiento automatizado de datos de carácter personal de 1981, a través del cual se fijaron principios específicos a tener en cuenta en el tratamiento de datos personales. A través de estos principios, se establece la protección necesaria a tener en cuenta en cada paso del tratamiento de datos desde su obtención, hasta su almacenamiento y difusión.

El Convenio de 1981 creó las bases para el nuevo derecho de protección de datos y estableció el nexo de unión entre este derecho y el derecho a la intimidad, basando la protección de los datos personales en la protección al derecho a la intimidad.

El objetivo de este Convenio fue fortalecer el derecho a la protección de datos, es decir, conferir una protección legal a los tratamientos automatizados de datos personales que se efectuaran. En este sentido, pretendía crear una serie de reglas que orientasen respecto a cómo debía ser tratada la información personal y cómo cada titular de los datos debería poder tener el control sobre tales tratamientos.

Posteriormente, los principios básicos del Convenio de 1981 fueron tenidos en cuenta en las tres principales directivas promulgadas en la Comunidad Europea sobre la materia:

- La Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.
- La Directiva 97/66/CE del Parlamento Europeo y del Consejo de 15 de diciembre, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las telecomunicaciones.
- La Directiva 2002/58/CE del Parlamento Europeo y del Consejo, de 12 de julio, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas.

La primera Directiva creó el primer marco regulatorio que permitía el libre movimiento de datos pero garantizando el respeto del derecho a la intimidad. En este sentido, reconocía que los avances continuos de carácter tecnológico desarrollados en los últimos tiempos habían generado nuevas formas de obtener, transmitir, manipular, grabar y almacenar datos personales. Por este motivo, fue redactada de una forma flexible con el fin de que pudiera ser fácilmente adaptada a los nuevos avances tecnológicos por suceder.

2 IPv6 y el derecho a la intimidad

La definición legal de "datos personales" se extendió hasta hacer referencia a *"cualquier información relativa a una persona física identificada o identificable (titular de los datos); se considerará identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un número de identificación o uno o varios elementos específicos, característicos de su identidad física, fisiológica, psíquica, económica, cultural o social"*. La relevancia de esta definición respecto al fenómeno IPv6 estriba principalmente en la referencia que realiza a un número como elemento de identificación.

La Directiva estableció reglas generales para el tratamiento de datos personales tales como el principio de calidad de los datos, los criterios para efectuar un tratamiento legítimo de datos, el deber de informar al titular de los datos; el derecho del titular de los datos a acceder a su información personal, su derecho de oposición, la confidencialidad y seguridad de los datos, notificaciones, el régimen sancionador, las transferencias internacionales de datos, los códigos de conducta y las autoridades de control.

Asimismo, el artículo 29 de la Directiva 95/46 creó un grupo independiente (Grupo del Artículo 29) cuya principal función es examinar, opinar, aconsejar y emitir recomendaciones relativas a cómo el tratamiento de datos personales podría impactar en los derechos y libertades de las personas.

Por otro lado, la Directiva 97/66 pretendió extender los principios consagrados en la Directiva 95/46 y aplicarlos al sector de las telecomunicaciones, como consecuencia del pronunciamiento de la Comisión por el cual establecía que en la actualidad *"están apareciendo nuevas redes digitales públicas avanzadas de telecomunicación que crean necesidades específicas en materia de protección de datos personales y de la intimidad de los usuarios, estando el desarrollo de la sociedad de la información caracterizado por la introducción de nuevos servicios de telecomunicaciones"*.

La utilización de nuevas redes de telecomunicaciones crea nuevos tipos de datos, los cuales no tienen por qué quedar claramente ubicados en los conceptos de "Datos personales" existentes hasta aquel momento. Por ello, esta Directiva se entendió como un medio para adecuar estas nuevas situaciones basadas en los novedosos avances tecnológicos a esta legislación vigente.

Sin embargo, esta Directiva rápidamente necesitó adaptarse a los nuevos cambios producidos en relación con el mercado y las tecnologías derivadas de los servicios de comunicaciones electrónicas, con el fin de aportar un nivel de protección en materia de protección de datos personales e intimidad equiparable al que existía para el sector de las comunicaciones electrónicas.

En este sentido, la Directiva 2002/58/CE fue promulgada como una respuesta a las nuevas tecnologías introducidas (por ejemplo redes digitales móviles), las cuales abrían un amplio abanico de posibilidades para los usuarios pero también importantes riesgos para su intimidad

y privacidad. Esta Directiva pretendió aportar seguridad a los usuarios garantizando que su intimidad no se vería puesta en riesgo como consecuencia de estos nuevos avances.

A pesar de ello, la Directiva 2002/58 no introdujo demasiados cambios respecto a la regulación de la anterior Directiva 97/66. Por el contrario, se dedicó a adaptarla y actualizarla a los nuevos desarrollos surgidos en el sector de las comunicaciones electrónicas. Por ello, esta nueva regulación pretendía unificar las telecomunicaciones, los medios y la tecnología de la comunicación y extenderse a toda la infraestructura de comunicaciones existente y a los servicios asociados con ésta siempre bajo la premisa de neutralidad tecnológica. La filosofía perseguida era la siguiente: el mismo servicio es regulado de la misma forma, independientemente de cómo es prestado o llevado a cabo.

El Considerando 6 de la Directiva 2002/58 establecía lo siguiente: *"Internet está revolucionando las estructuras tradicionales del mercado al aportar una infraestructura común mundial para la prestación de una amplia gama de servicios de comunicaciones electrónicas. Los servicios de comunicaciones electrónicas disponibles al público a través de Internet introducen nuevas posibilidades para los usuarios, pero también nuevos riesgos para sus datos personales y su intimidad."*

En conclusión, las tres mencionadas Directivas pretendían asegurar la existencia de protección suficiente en lo que a tratamientos automatizados de datos se refiere, fuera la tecnología que fuera a través de la cual se realizaran dichos tratamientos. Internet y, por lo tanto, IPv6, quedaron sometidos a las reglas y principios recogidos en estas Directivas(1).

La adecuación de estas tres directivas al fenómeno de IPv6 será tratado con mayor detenimiento en apartados posteriores de este libro. No obstante, es importante adelantar que los principios fundamentales existentes en materia de protección de datos personales son los siguientes:

- Obtención legal y legítima de los datos personales
- Uso de los datos únicamente para las finalidades de tratamiento identificadas inicialmente
- Datos adecuados, pertinentes y no excesivos
- Datos actualizados, reales y exactos
- Datos accesibles para su titular
- Mantenimiento de los datos en condiciones seguras
- Datos borrados o cancelados una vez que dejen de ser necesarios

Por lo tanto, aquellas entidades involucradas en el diseño y desarrollo de IPv6 deberán tener en cuenta estos principios para asegurar que, desde el inicio, se garantiza su respeto, el cual debe continuar durante el funcionamiento de este Protocolo.

(1) Documento del Grupo del Artículo 29 sobre el Tratamiento de Datos Personales en Internet de fecha 23 de febrero de 2003.

IPv6 y el derecho a la intimidad

3. ¿Cuáles son algunos de los principales aspectos de la intimidad en relación con Internet?

3.1. ¿Dónde están los peligros del Nuevo Protocolo de Internet?

Para conocer cuáles son los principales peligros para la intimidad en relación con Internet y con IPv6, es necesario conocer previamente cómo funciona Internet. En este sentido, Internet es una gran red de ordenadores comunicados los unos con los otros a través del Protocolo TCP/IP. A través del Protocolo IP, los ordenadores son capaces de comunicarse entre sí, estando cada uno de ellos identificado por una única dirección IP (en IPv4 esta dirección estaba compuesta por 32 bits y en IPv6 por 128).

El hecho que convierte IPv6 en un posible problema para la intimidad y la protección de datos parte de la necesidad de conocer si una dirección IP puede ser un dato personal, lo cual será analizado en el apartado 2.2. del Capítulo III de este libro.

En concreto, si una dirección IP es considerada como un dato personal en sí, entonces el tratamiento de estos datos personales estará protegido por las normas que regulan el derecho a la intimidad y la protección de datos y que han sido tratadas anteriormente.

3.2. Entidades con participación en Internet

Existen numerosos participantes en Internet, entre los cuales se pueden destacar los siguientes:

- Las industrias de software, ordenadores y telecomunicaciones que diseñan las redes de servicios disponibles.
- Los operadores de telecomunicaciones que proporcionan la red para la transferencia de datos.
- Los proveedores de acceso a Internet responsables del sistema de trasporte de Internet
- Los Proveedores de servicios de Internet, que proporcionan servicios como HTTP (a menudo como el ISP).
- Los usuarios.

Cada uno de estos participantes tiene su propia responsabilidad con respecto a la protección de datos y respeto a la intimidad y debe observar sus competencias así como el servicio que proporciona para asegurarse de que sus acciones cumplen con la normativa vigente aplicable.

Un informe publicado por el Grupo Internacional de Protección de Datos en Telecomunicaciones ("Budapest - Berlin Memorandum on Data Protection and Privacy on the Internet") de 1996, proporciona una visión general de la Privacidad en Internet que afecta a Internet en general.

Dicho documento explica que el vasto crecimiento de Internet había creado lo que había sido denominado como el primer nivel de la emergente Infraestructura Global de Información (IGI) que potencialmente causaba numerosos problemas en relación con la privacidad. Existen varios participantes en Internet y cada uno cuenta con diversas tareas, intereses y oportunidades y los principios de privacidad y de protección de datos deben ser observados en todos esos diferentes estadios.

"Considerando que Internet no está bajo un solo órgano regulador que supervise todos los aspectos de la privacidad y la protección de datos a una escala global, el usuario está obligado a confiar en la seguridad de toda la red, que es cada componente de la misma, con independencia de donde se encuentre localizado o por quien esté dirigido".

El documento establece que hay ciertas entidades (internacionales, regionales o nacionales) que dirigen varias funciones en la Red y considerando el hecho de que no existe un órgano de gobierno para Internet, el papel de estas entidades es importante, en particular cuando se desarrollan los protocolos y los estándares para Internet, se fijan reglas para la identificación de los servidores conectados y eventualmente para la identificación de los usuarios. Esto es directamente aplicable al contexto de IPv6.

"Debe encontrarse un equilibrio entre la persona que no quiere dejar sus huellas en la Red y el hecho de que los proveedores necesiten su identificación y autenticación para ayudar con las tareas de marketing y de tarificación".

3.3. Pautas para el respeto a la Privacidad

El mencionado Grupo de Protección de Datos en las Telecomunicaciones publicó un plan de 10 puntos con una visión general de los principios que deben tenerse en cuenta en estas materias.

El plan de 10 puntos establece:

"*No puede haber duda de que la protección legal y técnica de la privacidad de los usuarios en Internet es actualmente insuficiente*".

Por una parte, el derecho de cada individuo para usar la información en Internet sin ser observado ni identificado debe estar garantizado. Por otra parte, debe haber límites (barreras) con respecto al uso de los datos personales por terceras personas en la Red.

Una solución al dilema básico debería ser fundada en los siguientes niveles:

1. Los proveedores de servicios deberían informar inequívocamente a cada potencial usuario sobre los riesgos para la privacidad existentes en la Red. El usuario debe hacer balance de los riesgos frente a los posibles beneficios.
2. En muchas circunstancias, la decisión de entrar en Internet y decidir cómo usarla, está sujeta a la regulación legal establecida para la protección de datos por cada Estado.

IPv6 y el derecho a la intimidad

3. Deben ser apoyadas las iniciativas para una mayor cooperación internacional, incluyendo una convención internacional que regule la protección de datos en el contexto de las redes internacionales y servicios.

4. Debe establecerse un mecanismo internacional de supervisión que debe ser construido sobre la base de las estructuras ya existentes tales como la Sociedad de Internet y otras entidades. La responsabilidad por la protección de la privacidad debe ser institucionalizada en cierta forma.

5. El derecho internacional y nacional debe establecer inequívocamente que el proceso de comunicación (vía correo electrónico) se encuentra protegido por el secreto de las telecomunicaciones.

6. Además es necesario desarrollar medios técnicos para mejorar la privacidad de los usuarios en la Red. Es obligatorio desarrollar principios para la información y las comunicaciones tecnológicas y multimedia, hardware y software, que habiliten al usuario para controlar el tratamiento de sus datos personales.

7. Los medios técnicos deben también ser usados para proteger la confidencialidad. El uso de los métodos de codificación deben constituirse y permanecer como una opción legítima para cada uno de los usuarios de Internet. El Grupo de Trabajo apoya los nuevos progresos del Protocolo de Internet (IPv6), que proporciona medios para mejorar la confidencialidad de la codificación, la clasificación de mensajes y una mejor autenticación de los procesos. Los productores de software deberían implementar los estándares de seguridad del nuevo Protocolo de Internet en sus productos y deberían proporcionar el uso de estos productos lo más rápido posible.

8. El Grupo de Trabajo aprobaría un estudio de la viabilidad para establecer un nuevo procedimiento de certificación que expida "sellos de calidad" para los proveedores y los productos, del tipo de un certificado de aprobación de la privacidad.

9. El anonimato es un valor adicional esencial para la protección de la privacidad en Internet. Las limitaciones al principio de anonimato deberían estar restringidas a lo que es estrictamente necesario en una sociedad democrática sin cuestionar tal principio.

10. Finalmente será decisivo descubrir como la "auto-regulación" a través de una "Netiqueta" y la tecnología protectora de la privacidad podrían mejorar la implementación de una normativa internacional y nacional de protección de la privacidad. No será suficiente con confiar en cada una de estas vías de acción: éstas deben estar combinadas de forma efectiva para alcanzar la Infraestructura Global de Información que respeta el derecho humano a la privacidad y a las comunicaciones inadvertidas".

El Grupo de Trabajo del Artículo 29, observando los aspectos fundamentales con respecto

a Internet, estableció unas directrices generales. En dicho artículo se determinaba que:

- *"Internet fue concebido como una red abierta a nivel de trabajo (www) a través de la cual la información podía ser compartida. Sin embargo, es necesario encontrar un equilibrio entre la "naturaleza abierta" de Internet y la protección de los datos personales de los usuarios de Internet (proporcionalidad).*
- *Una gran cantidad de datos personales de los usuarios de Internet son recopilados a través de las páginas de Internet pero, sin embargo, a menudo los usuarios no son conscientes de este hecho. Esta falta de transparencia hacia los usuarios necesita ser redirigida para alcanzar un óptimo nivel de protección de los usuarios.*
- *Los protocolos son medios técnicos a través de los cuales se establece cómo los datos deben ser recogidos y procesados. Los programas software y navegadores web juegan también un papel importante ya que, en algunos casos, incluyen un identificador que hace posible relacionar un usuario de Internet con las actividades que ha realizado en la Red. Por lo tanto, es responsabilidad de aquellos que se encuentran involucrados en el diseño y el desarrollo de estos productos, el ofrecer a estos usuarios las soluciones que permitan cumplir con la normativa de protección de la privacidad de los usuarios".*

La cuestión del anonimato ha sido específicamente tratada en la Recomendación 3/97 sobre Anonimato en Internet de 3 de diciembre de 1997, en la cual se establece que:

"A lo largo de los últimos 25 años, se ha ido haciendo patente que una de las mayores amenazas que pesan sobre el derecho fundamental a la intimidad es la capacidad que tienen algunas organizaciones de acumular gran cantidad de información sobre los particulares, en forma digital, que permite su manipulación, alteración y transmisión a terceros con enorme rapidez (y actualmente a un coste muy bajo). La inquietud que suscita esta evolución y la posibilidad de que se haga uso indebido de tales datos personales ha llevado a todos los Estados miembros de la UE (y ahora a la Comunidad, con la Directiva 95/46/CE) a adoptar disposiciones específicas sobre protección de datos en las que se establece un marco normativo que regula el tratamiento de la información de carácter personal".

Una característica de las redes de telecomunicaciones, y de Internet en particular, es su capacidad de generar una ingente cantidad de datos transaccionales (datos generados a fin de asegurar conexiones correctas). La posibilidad de utilizar las redes de modo interactivo (característica específica de numerosos servicios de Internet) hace aumentar aún más la cantidad de datos transaccionales.

A medida que evolucionen los servicios en línea, aumentando su complejidad y su popularidad, irá adquiriendo más importancia el problema de los datos transaccionales.

IPv6 y el derecho a la intimidad

Sea cual sea el lugar al que se acceda en Internet, se deja un rastro digital, de manera que, al ser cada vez mayor el número de actividades de nuestro quehacer cotidiano que se realizan en línea, irá aumentando la información que sobre nuestras ocupaciones, gustos y preferencias quede registrada.

Los datos transaccionales sólo suponen una amenaza a la intimidad de las personas si se refieren a alguien identificado o identificable. Es evidente, por tanto, que una manera de conjurar esta amenaza consistiría en cerciorarse de que, siempre que sea viable, los rastros creados al utilizar Internet no permitan identificar al usuario. De garantizarse el anonimato, cualquiera podrá participar en la revolución de Internet sin temor a que queden registrados todos sus movimientos y a que se acumule información sobre su persona que pueda utilizarse más adelante con fines contrarios a su voluntad."

Sin embargo, el principio de anonimato debe estar equilibrado con el "principio de proporcionalidad". La Recomendación se refiere al punto fundamental del anonimato, considerando que debe aplicarse la misma regla de comportamiento que fuera de la Red, a las actividades realizadas a través de la misma.

Finalmente la Recomendación concluye que:

"*La posibilidad de mantener el anonimato es fundamental para que la intimidad de las personas goce de la misma protección en línea que fuera de línea*". Sin embargo, esto debería estar siempre equilibrado, teniendo en cuenta otras consideraciones como la prevención de delitos.

Además, en relación con los Protocolos de Internet y, por lo tanto, con IPv6, la Recomendación establece que:

"El acceso de los usuarios y las actividades desarrolladas en Internet son raramente anónimas (...), la configuración técnica de los Protocolos de Internet no hace posible en realidad el anonimato (...)".

Internet plantea un problema porque *"el uso de la infraestructura está a menudo directamente basado en el tratamiento de los datos personales, del tipo de ciertas direcciones IP".*

4. ¿En qué afecta específicamente IPv6 a la privacidad?

Como se ha mencionado, a finales de los 90, surgieron comentarios acerca de la preocupación sobre los aspectos fundamentales de la privacidad en relación con IPv6 en los Estados Unidos y estas preocupaciones fueron trasladadas a las autoridades europeas.

El primer documento oficial fue emitido cuando la Comisión Europea publicaba la Comunicación 96 (COM, 2002), de 21 de febrero 2002. Esta publicación era una comunicación de la Comisión

IPv6 y el derecho a la intimidad

al Consejo y al Parlamento Europeo titulada "Next Generation Internet – priorities for action in migrating to the new Internet protocol IPv6". La finalidad de este documento fue definir los puntos de vista y las inquietudes de la Comisión Europea referentes al desarrollo de IPv6 en Europa y uno de sus principales aspectos era el tema de la privacidad.

El pensamiento de la Comisión Europea queda claramente recogido en el siguiente párrafo:

"Sin embargo, para que la nueva versión de Internet habilite servicios que puedan ser realizados de forma oportuna, es fundamental estructurar, consolidar e integrar los esfuerzos europeos en IPv6, y notablemente desarrollar los medios humanos cualificados para armonizar completamente, cuando sea necesario, los enfoques en las políticas, para mantener los desarrollos alcanzados, promover los estándares y las especificaciones de trabajo y asegurar que todos los sectores de la nueva economía probablemente afectada por IPv6 sean totalmente conscientes de los potenciales beneficios que pueden derivarse de su adopción."

Asimismo, la Comisión propone una serie de acciones para asegurar que la Unión Europea mantenga la iniciativa y el liderazgo en estos progresos globales. Estas acciones requieren una acción concertada encaminada a la estructuración, consolidación e integración de los esfuerzos europeos en IPv6, notablemente a través de:

1. Un apoyo cada vez mayor de IPv6 a través de las redes y servicios.
2. El establecimiento y lanzamiento de programas educacionales de IPv6.
3. La estimulación continua del establecimiento de Internet a través de Europa.
4. La adopción de IPv6 a través de la concienciación promovida por campañas.
5. Un apoyo cada vez mayor de las actividades de IPv6, en el sexto Programa Marco.
6. La consolidación del apoyo para permitir redes de investigación a nivel nacional y europeo.
7. Una contribución activa para la promoción de los estándares de trabajo de IPv6.
8. La integración de IPv6 en todos los planes estratégicos concernientes al uso de los nuevos servicios de Internet.

Habiendo sentado las bases, la Comunicación específicamente trata los aspectos fundamentales de la privacidad en relación con IPv6.

"Debido al hecho de que desde sus inicios, Internet ha sido considerado como una red abierta, hay muchas características de sus protocolos de comunicación que, más por accidente que por diseño, pueden conducir a una invasión de la privacidad de los usuarios de Internet. El derecho fundamental a la privacidad y a la protección de los datos personales es recogido en la Carta de Derechos Fundamentales de la UE y desarrollado en detalle

en las Directivas 95/46/CE y 97/66/CE sobre protección de datos personales, las cuales son aplicables al tratamiento de los datos personales en Internet. En su Comunicación sobre la organización y la dirección de los sistemas de dominios en Internet de abril de 2000, la Comisión ya establecía que la dirección IP puede ser un dato personal. Así el Grupo del Artículo 29, el cuerpo asesor independiente de la UE para la protección de datos personales y la privacidad, establecía que la Directiva 95/46/CE llama la atención en numerosas ocasiones a aspectos derivados de la privacidad por el uso de Internet. El Grupo del Artículo 29 así como el Grupo de Trabajo Internacional para la protección de los datos personales en las telecomunicaciones (El "Grupo de Berlín") trabajan especialmente en IPv6.

Por lo tanto, es indispensable que la Comisión Europea y la Unión Europea como una sola entidad consideren los aspectos fundamentales relacionados con la privacidad en el desarrollo de Internet. Mientras que los aspectos fundamentales de la privacidad están siendo considerados en el desarrollo de IPv6, es esencial que la confianza de los usuarios de Internet en todo el sistema, incluyendo el respeto de sus derechos fundamentales, esté siendo asegurada".

En sus conclusiones, la Comisión Europea pidió a las partes:

"Estudiar el impacto de una mayor evolución de Internet incluyendo la nueva generación del Protocolo IPv6, sobre los derechos fundamentales de la privacidad y de la protección de datos personales, para conseguir asegurar que los estándares y las especificaciones necesarias tengan en cuenta estos aspectos en su totalidad".

Habiendo hecho una llamada para el estudio general sobre estos aspectos, pocos meses después, en mayo de 2002, el Grupo del Artículo 29 publicaba un documento llamado "Opinion 2/2002 on the use of unique identifiers in telecommunications terminal equipment: The example of IPv6."

Este documento remarca el peligro que supone para la privacidad *"la posibilidad de la integración de un único número identificador en la dirección IP diseñado de acuerdo al nuevo protocolo".*

La idea central de este documento es que la dirección IP atribuida a los usuarios de Internet podría ser considerada como un dato personal y, por lo tanto, estaría sujeta a las Directivas establecidas por la Unión Europea.

5. ¿Cuál es el fundamento para esta preocupación sobre la privacidad?

Las preocupaciones acerca de la privacidad remarcadas en la sección 4 están fundadas en el formato de creación de direcciones IPv6, aprobado por el Internet Engineering Task Force (IETF). Este es el cuerpo técnico que asesora acerca de cómo Internet debe ser desarrollado y establece los estándares para Internet a través de la publicación de varios estándares técnicos conocidos como RFCs.

IPv6 y el derecho a la intimidad

5.1. Petición de Comentarios

Los RFC son una serie de documentos generados en base a un conjunto de notas técnicas y organizativas acerca de Internet. En ellos se discutían varios aspectos de la red de ordenadores, incluyendo protocolos, procedimientos, programas y conceptos. Estos específicos documentos no oficiales del protocolo de Internet consiguieron una importancia creciente y fueron recogidos y publicados como los estándares RFCs.

Este hecho desencadenó la consideración de los RFC's como estándares no oficiales a través de los cuales se determinaba cómo Internet debía ser desarrollado. En este sentido, la publicación de RFC's se convirtió en un paso fundamental para el proceso de creación de estándares definitivos y reconocidos.

En concreto, los RFC's deben publicarse previamente como borradores con el fin de que los expertos en las áreas involucradas tengan la posibilidad de formular los comentarios que consideren oportunos, con carácter previo a que se llegue a un consenso y el RFC se convierta en un estándar.

En este sentido, el proceso es el siguiente: la especificación en concreto entra en un periodo de desarrollo y creación tras el cual queda sometida a la revisión por los expertos correspondientes hasta que finalmente pasa a considerarse un estándar.

Por lo tanto, es posible destacar 3 niveles distintos en un RFC:

- Propuesta de estándar
- Borrador de estándar
- Estándar

5.2. ¿Tienen Identificadores Únicos las direcciones basadas en IPv6?

Existen numerosos tipos de direcciones IP basadas en IPv6 pero la posible colisión con la privacidad e intimidad se encuentra en los supuestos de autoconfiguración de las direcciones sin estado.

Los aspectos técnicos sobre esta materia se encuentran especificados en los siguientes documentos: RFC2373 (arquitectura de direccionamiento IPv6), RFC2642 (autoconfiguración de direcciones IPv6 sin estado) y RFC2374 (formato agregable de direcciones IPv6 globales de unidifusión), así como en posterior documentación existente sobre esta materia (draft-ietf-ipv6-unicast-aggr-v2-02.txt).

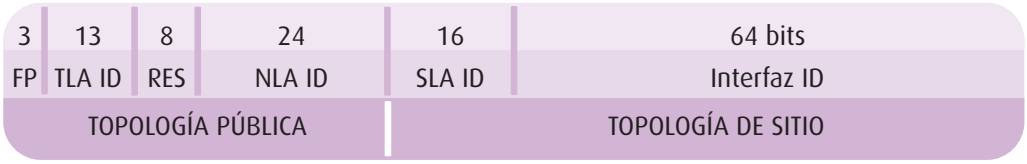
IPv6 y el derecho a la intimidad

En este apartado no se pretende profundizar en los aspectos técnicos de la creación y composición de estas direcciones pero sí explicar en términos sencillos cómo son creadas y cómo esto afecta en términos de privacidad.

El principal objetivo de la autoconfiguración de direcciones sin estado (Stateless Address Autoconfiguration) es generar una dirección global única sin la necesidad de un DHCP (Dynamic Host Configuration Protocol). DHCP es el protocolo que permite a un administrador de redes supervisar, gestionar y asignar las direcciones IP.

A los efectos de conocer cómo se organiza una dirección basada en IPv6, se pone un ejemplo a continuación. Utilizando la analogía del correo postal, lo normal es poner el nombre del destinatario, seguido de la dirección, ciudad, estado, código postal y el país.

Este estándar se encuentra actualmente aceptado y utilizado en el envío de correspondencia postal tradicional. En este sentido, existe un estándar parecido a seguir para las direcciones IPv6 con el fin de distribuir los 128 bits.



Formato agregable de direcciones IPv6 globales de unidifusión

Los números de la primera fila de la tabla hacen referencia a los "bits". Cada uno de los "bits" está relacionado con una capa diferente que permite la comunicación en la red. La dirección se divide en dos partes: topología pública y topología de sitio.

La topología de sitio será "privada" dependiendo del tipo de red individual y la topología pública hará referencia a la red pública que permite la comunicación por Internet.

Asimismo, cada una de las partes principales recogidas en la figura, se explican a continuación:

FP: Prefijo de Formato. Su valor es 001.

TLA ID: Top Level Aggregation Identifiers, se encuentra en el nivel superior de la jerarquía de encaminado. La topología del encaminado a todos los niveles debe ser diseñada para minimizar el número de rutas en la tabla de encaminado. Cada organización a la que le es asignado un TLA ID recibe 24 bits de espacio NLA ID. Este espacio puede ser delegado aproximadamente a tantas organizaciones como en el actual Internet IPv4. Las organizaciones a las que se ha asignado un TLA IP pueden proveer servicios a organizaciones que proporcionan servicios de tránsito público y a organizaciones que no lo proporcionan. Las organizaciones que reciben un NLA ID pueden incluso optar por delegar su espacio a otro NLA ID.

IPv6 y el derecho a la intimidad

RES	Espacio reservado para el futuro y debe dejarse en cero.
NLA ID	Next Level Aggregation Identifier es utilizado en organizaciones con TLA ID para crear una jerarquía de direccionamiento y para identificar sitios. La organización puede asignar la parte superior del NLA ID para crear una jerarquía de direccionamiento apropiada para la red en cuestión.
SLA ID	Site-Level Aggregation Identifier. El campo SLA ID es usado por una organización individual para crear su propia jerarquía de direcciones local y para identificar subredes. Es un campo de 16 bits y soporta 65.535 subredes. La selección realizada para estructurar un campo SLA ID es responsabilidad de cada organización individual.
Interface ID	Los identificadores de interfaz son números de serie únicos o direcciones que están vinculadas al enlace y, por lo tanto, son utilizados para identificar interfaces en un enlace. Estos identificadores deben ser únicos para el enlace en cuestión. Esta es la parte de las direcciones que podría causar problemas de privacidad. En concreto, un interfaz es definido como un vínculo de un nodo a un enlace. Los identificadores de interfaz son números de serie únicos o direcciones vinculados al enlace. Un identificador para un interfaz es único para cada enlace (al menos).

Esta explicación puede simplificarse a través de la siguiente figura:

Actualización del formato agregable de direcciones IPv6 globales de unidifusión

IPv6 utiliza los 128 bits para generar el direccionamiento, encaminado y la información de identificación en el interfaz de un ordenador o en una tarjeta de red. Algunos sistemas basados en IPv6, usan los 64 bits de la parte derecha del gráfico para almacenar un identificador global IEEE (EUI64). Este identificador se compone de unos valores ID de entidad asignados a un fabricante por la Autoridad de Registro IEEE. Los 64 bits que conforman un identificador son una concatenación de la identificación de la entidad de 24 bits y del identificador de extensión de 40 bits asignado por la organización con la entidad de asignación de identidades. La dirección MAC de 48 bits de un interfaz de una tarjeta de red podrá también ser usada para generar el EUI64.

Los problemas relacionados con la privacidad nacieron en base a estos Identificadores de Interfaz (Interface ID), los cuales están basados en el ID del interfaz del hardware, tal y como

se ha descrito anteriormente, de manera que podrían identificar individualmente a cada máquina. Por lo tanto, cada vez que se accede a Internet para enviar o recibir paquetes de información, este hecho deja una huella siempre, la cual podrá ser rastreada hasta conocer el usuario de la máquina.

5.3. ¿Cómo se configura una dirección IPv6?

El RFC2642 explica como la autoconfiguración de direcciones sin estado combina un identificador de interfaz con un prefijo para formar una dirección.

El RFC establece lo siguiente:

"Este documento especifica los pasos a seguir por un servidor para decidir cómo autoconfigurar sus interfaces a través de la versión 6 del protocolo IP. El proceso de autoconfiguración incluye la creación de una dirección de enlace local y la verificación del carácter único para ese enlace, determinando qué información debería ser autoconfigurada (direcciones, otra información o ambos), y en el caso de direcciones, si éstas son obtenidas a través de un mecanismo sin estado, a través de un mecanismo con estado o por ambos. Este documento determina el proceso para generar esta dirección de enlace local, el proceso para generar las direcciones globales a través de una autoconfiguración de direcciones sin estado y el procedimiento de detección de direcciones duplicadas (DAD, Duplicate Address Detection)."

"Uno de los principales objetivos de la autoconfiguración sin estado es la siguiente:

- *No sería necesario la configuración manual de máquinas de forma individual con carácter previo a conectarlas a la red. En consecuencia, se necesitará algún mecanismo que permita a una máquina obtener o crear direcciones únicas para cada uno de sus interfaces. La autoconfiguración de direcciones conlleva que cada interfaz puede generar un identificador único para dicho interfaz (un "identificador de interfaz"). En el supuesto más sencillo, un identificador de interfaz hace referencia a la capa de enlace de la dirección del interfaz. Un identificador de interfaz puede combinarse con un prefijo para generar una dirección."*

En resumen, este RFC subraya cómo este tipo de direcciones basadas en IPv6 son generadas por ellas mismas en lugar de ser asignadas y se encuentran basadas en identificadores únicos en el hardware.

5.4. ¿Cuál es el problema con la autoconfiguración de direcciones sin estado?

El potencial problema de cara a la privacidad que podría surgir con este tipo de direcciones se encuentra claramente especificado en el RFC3041. Este documento pone de manifiesto que cualquier sistema de comunicación que se base o utilice una dirección fija o un identi-

ficador tanto para recibir como para enviar información, conlleva problemas potenciales en materia de privacidad (este problema ya existía para IPv4, no siendo específico de IPv6).

"La autoconfiguración de direcciones sin estado define cómo un nodo basado en IPv6 genera direcciones sin necesitar un servidor DHCP. Algunos tipos de interfaces de red tienen un identificador IEEE embebido (una dirección MAC, en la capa de enlace). En estos casos, la autoconfiguración de direcciones sin estado usa el identificador IEEE para generar un identificador de interfaz de 64 bits. Por diseño, el identificador de interfaz es único cuando se genera de esta forma. El identificador de interfaz se une a un prefijo para componer una dirección IPv6 de 128 bits.

Todos los nodos combinan identificadores de interfaz (ya sean generados a través de un identificador IEEE o través de cualquier otra técnica) con el prefijo link-local reservado para generar direcciones link-local para sus interfaces vinculados. En consecuencia, las direcciones adicionales, incluyendo las direcciones de ámbito local, son creadas mediante la combinación de prefijos señalados en los anuncios de rutas (Router Advertisements) a través del descubrimiento de vecindario (Neighbour Discovery) con el identificador de interfaz.

Sin embargo, no todos los nodos e interfaces contienen identificadores IEEE. En estos casos, los identificadores se generan a través de otros medios (por ejemplo, aleatoriamente), y el identificador resultante no es único de forma global y podrá cambiar con el tiempo. El propósito de este documento (RFC3041) está basado en las direcciones generadas con identificadores IEEE, ya que sólo se da la problemática en materia de privacidad cuando existen identificadores únicos que, además, no cambian con el tiempo".

El propio RFC3041 pone de manifiesto el potencial problema en materia de privacidad, derivado del uso de identificadores únicos como partes constantes de las direcciones.

El uso de identificadores de interfaz no cambiantes para componer direcciones es un caso específico fuera de los casos más generales donde el identificador es reutilizado a lo largo de un determinado periodo de tiempo y en actividades múltiples y distintas. En los casos en los que el mismo identificador es utilizado en múltiples contextos, nace la posibilidad de que dicho identificador sea utilizado para relacionar otras actividades no vinculadas hasta ese momento. Por ejemplo, un sniffer colocado estratégicamente en un lugar por donde pasa el tráfico tanto de entrada como de salida hacia un nodo o servidor, podrá mantener un seguimiento acerca de los destinos con los que un nodo está comunicándose y sobre el momento en el que se produce esa comunicación. Esta información podrá ser interesante y ser utilizada para otros propósitos, por ejemplo, conocer las horas en las que un empleado se encuentra trabajando, las horas durante las que una persona estuvo en su casa, etc.

Los navegadores web y los servidores frecuentemente se intercambian entre sí "cookies" que pueden permitir a los servidores web relacionar una actividad que se está llevando a cabo con otra anterior. En este sentido, una de las actividades más comunes que se está realizando

es enviar publicidad a un usuario utilizando la cookie del navegador web para identificar qué consultas o actividades se solicitaron con anterioridad. En este caso, tomando como referencia la información aportada por las cookies, resulta mucho más sencillo enviar publicidad que se adapte con mayor precisión a los gustos y preferencias del usuario en cuestión.

El uso de un identificador constante en una dirección es especialmente importante porque las direcciones son un elemento fundamental para que exista la comunicación y no es fácil mantenerlas escondidas o preservadas de rastreadores o terceros. Incluso en los supuestos en los que las capas superiores codifiquen sus informaciones, las direcciones en los encabezados del paquete siguen apareciendo en claro. En consecuencia, si un dispositivo móvil (como un ordenador portátil) accede a la red desde distintos puntos, cualquier rastreador será capaz de seguir sus movimientos de un lugar a otro, incluso en el supuesto de que las informaciones de las capas superiores de la dirección se encuentren codificadas.

5.4.1. Algunos aspectos relevantes relacionados con las direcciones IPv6

La división de las direcciones de IPv6 en distintas topologías e identificadores podría suponer que una porción fija de una dirección de IPv6 (un identificador de interfaz) podría contener un identificador que permanezca constante incluso cuando la topología de la dirección cambie (como en el caso resultante de conectarse desde otro punto de Internet). Por el contrario, con IPv4, cuando parte de una dirección cambiaba, conllevaba el cambio de la dirección completa (incluyendo la parte local de la dirección).

En este sentido, si las direcciones fueran generadas en base a un identificador de interfaz, la dirección utilizada por un usuario desde su casa contendría un identificador único, el cual se mantendría igual en una sesión que en otra, a pesar de que se modificara el resto de la dirección.

Sin embargo, un supuesto más problemático es el de los dispositivos móviles (portátiles, PDAs, etc.) los cuales pueden moverse y conectarse desde distintos puntos a Internet. En cada supuesto en el que estos dispositivos se mueven (y en los casos en los que no dispongan de tecnología basada en movilidad IP), estos dispositivos crearían sus propias direcciones en base a su punto de enganche actual.

Mientras que la dirección del dispositivo cambia cuando éste se mueve, en todo caso, el identificador único existente en la dirección se mantiene igual. En este caso, el identificador podrá ser utilizado para rastrear el movimiento y el uso de una máquina o dispositivo concreto. Por ejemplo, un servidor que almacena el uso de la información así como la dirección de origen también estará almacenando el identificador único ya que éste estará incluido en la dirección. En consecuencia, cualquier actividad de data-mining a través de la cual se puedan relacionar actividades efectuadas con las direcciones a través de las cuales se llevaron a cabo, también serán de aplicación en los supuestos en los que existan identificadores únicos en las direcciones.

6. ¿Tienen solución estos problemas relacionados con la privacidad?

6.1. RFC3041 - Problemas de Privacidad en la Autoconfiguración de direcciones sin estado con IPv6

El RFC3041 "Privacy Extensions for Stateless Address Autoconfiguration in IPv6" es un estándar técnico que se considera, en la actualidad, como una posible solución de naturaleza técnica a los posibles riesgos que, respecto a la privacidad y la protección de datos de los usuarios, podrían existir como consecuencia del uso del nuevo Protocolo IPv6.

Este RFC establece un sistema de dos direcciones: una dirección que es la utilizada para recibir comunicaciones, de manera que la interfaz del terminal es siempre localizable a través de la dirección permanente y otra dirección generada aleatoriamente utilizada por el terminal para las comunicaciones salientes. De esta manera, a través del RFC3041, en líneas generales, cuando las comunicaciones son generadas por el usuario, su dirección IP no sería rastreable por terceros.

En este sentido, el RFC3041 así como su funcionamiento y utilidades serán analizados en el Capítulo III de este libro.

7. Conclusiones

A continuación, se enumeran las principales conclusiones de este estudio acerca de las implicaciones, en materia de privacidad, de la utilización del nuevo Protocolo IPv6:

1. Mientras que se produce el rápido desarrollo de IPv6 y éste se potencia, es importante no olvidar que debe efectuarse salvaguardando determinados principios esenciales.
2. El derecho a la intimidad y, como consecuencia, el derecho a la protección de datos son derechos reconocidos en la legislación vigente siendo, por tanto, su respeto y cumplimiento una obligación esencial.
3. Si bien la tecnología se desarrolla y avanza con gran velocidad, la legislación europea pretende facilitar una serie de elementos para verificar su cumplimiento y garantizar la protección del derecho a la intimidad a lo largo de todos los pasos existentes en la implementación de cualquier nueva tecnología.
4. En líneas generales, los desarrolladores de nueva tecnología y protocolos deben tener en mente la obligación de respetar el derecho a la intimidad y los principios de protección de datos. En este sentido, ambos derechos reconocen la posibilidad de que los ciudadanos sean anónimos a pesar de que esta posibilidad se vea limitada por ciertas facultades que, por ejemplo, disponen las fuerzas policiales en orden a prevenir actividades ilegales.

Protección de datos personales

1. Introducción

Una las razones que motivan el estudio sobre protección de datos objeto de este Capítulo, se deriva del hecho de que la legislación de protección de datos, a nivel general, va consolidándose y siendo conocida tanto por las empresas, como por los organismos públicos y por los ciudadanos, los cuales se encuentran adquiriendo, a medida que pasa el tiempo, una sensibilización y un conocimiento amplio acerca de cuáles son sus derechos y obligaciones conforme a esta normativa.

Este hecho, sin duda, es otro de los principales motivos que obligan a tener en cuenta cualquier aspecto que pudiera afectar a la implantación y uso de IPv6 sobre esta materia, de forma que se potencie la consideración de este Protocolo como un elemento seguro y que aporte confianza a sus potenciales usuarios.

El objeto de este Capítulo, si bien está estrechamente unido con el derecho a la intimidad o privacidad, es analizar las posibles implicaciones que IPv6 podría tener en materia de protección de datos personales, como consecuencia de la posible consideración de las direcciones IP como datos de esta naturaleza, en determinadas ocasiones, como ya ha venido apuntándose en Capítulos anteriores.

En este sentido, conviene aclarar que si bien la protección de datos personales suele entenderse incluida dentro de la amplia esfera que constituye el derecho a la intimidad o privacidad de las personas, es una rama específica que se centra en asegurar que los tratamientos o usos a los que se destinen los datos personales de una persona física, se efectúen conforme a la legalidad existente.

Por lo tanto, este Capítulo se centra, en primer lugar, en analizar la legislación actual existente a nivel europeo en materia de protección de datos personales, a los efectos de poder discernir si ésta contempla y regula las posibles problemáticas que pudieran surgir como consecuencia de la implantación de IPv6 o si, por el contrario, se hace necesaria su modificación o adaptación a este Protocolo.

Asimismo, será objeto de este Capítulo, identificar algunos supuestos problemáticos derivados de la implantación de IPv6, en relación con la normativa de protección de datos así como la aplicabilidad de ciertas soluciones técnicas que se han venido desarrollando al objeto de preservar la intimidad de los usuarios de este Protocolo, en concreto, los aspectos relacionados con el RFC3041.

Para finalizar, se realizará una breve referencia al problema de la extraterritorialidad y, por tanto, de la dificultad de llegar a una única legislación que solucione la problemática nacida en Internet en relación con la regularización de determinadas conductas y, en el caso que nos ocupa, la unificación de criterios respecto al tratamiento de datos personales,

siendo necesario asegurar la armonización de las legislaciones existentes sobre estas materias a nivel mundial, a los efectos de lograr un nivel razonable de seguridad jurídica y de unificación de criterios.

2. ¿Qué es la Protección de Datos de Carácter Personal?

2.1. Concepto de Protección de Datos Personales

A través del concepto "protección de datos personales" actualmente se viene definiendo, de forma comúnmente aceptada, un derecho fundamental de toda persona física, también conocido como el "derecho a la autodeterminación informativa".

Este derecho hace referencia al amparo que debe ofrecerse y garantizarse a los ciudadanos como consecuencia del tratamiento de sus datos o informaciones de naturaleza personal por parte de terceros y de forma no autorizada. En definitiva, *es "la protección jurídica de las personas en lo referente al tratamiento automatizado de los datos de carácter personal que las conciernen".*

En este sentido, la necesidad de garantías de esta naturaleza se ha visto potenciada como consecuencia del avance de las nuevas tecnologías que permiten el tratamiento de datos personales por numerosos agentes y en una gran diversidad de situaciones, lo cual, a priori, podría crear una cierta inseguridad por parte de las personas físicas, titulares de tales datos.

Por todo ello, el derecho a la protección de datos permite a los titulares de los datos poder decidir qué puede realizarse con sus datos y obtener las garantías suficientes de que dicho tratamiento se efectuará siempre dentro del marco de la legalidad.

En este sentido, la Carta de Derechos Fundamentales adoptada el 8 de Diciembre del 2000 de la Unión Europea, en su artículo 8 reconoce el derecho de todos los ciudadanos a la protección de sus datos personales, de manera que el tratamiento de los mismos debe ser acorde a los motivos expuestos y siempre amparado en el consentimiento del titular o en la ley.

2.2. Consideración de la Dirección IP como un dato de carácter personal

A continuación, como ya se viene apuntando a lo largo de otros capítulos, se pretende determinar si una dirección IP puede ser considerada como un dato de carácter personal para lo cual, con carácter previo, se expondrán una serie de conceptos básicos que deberán ser tenidos en cuenta.

En este sentido, el pionero Convenio de 28 de enero de 1981 del Consejo de Europa (conocido como el Convenio 108) definía dato personal de la siguiente forma genérica: *"cualquier información relativa a una persona física identificada o identificable".*

Protección de datos personales

Asimismo, la propia Directiva 95/46/CE en su artículo 2 (a) considera como dato personal "*cualquier información relativa a una persona identificada o identificable como, por ejemplo, los datos de carácter numérico o cualquier información característica de su identidad física, psíquica, económica, cultural o social".*

En consecuencia, a través de esta definición, pueden extraerse dos elementos esenciales que deben existir para poder considerar cierta información como un dato de carácter personal:

- El titular del dato debe ser siempre una persona física, no una persona jurídica.
- Posibilidad de asociar esta información de cualquier naturaleza, con esa persona física, bien directa o indirectamente.

Dicho esto, cabe deducirse que siempre que cualquier información sea posible relacionarla con una persona física que ya se encuentre identificada o que pueda serlo en el futuro (a través de medios razonablemente posibles), se entenderá que dicha información es un dato personal y, por lo tanto, su tratamiento deberá efectuarse conforme a las exigencias determinadas por la legislación vigente en la materia.

El Considerando 26 de dicha Directiva establece que para determinar si una persona es identificable, hay que tener en cuenta el conjunto de los medios que puedan ser razonablemente utilizados por el responsable del tratamiento o por cualquier otra persona, para identificar a dicha persona.

Asimismo, otro de los conceptos esenciales a la hora de comprender esta normativa, es el concepto de tratamiento de datos personales. En este sentido, es importante resaltar que lo que realmente está regulado por esta normativa es el hecho de que se efectúe un tratamiento con los datos personales. El mero hecho de ser titular de los mismos, en principio, no confiere al sujeto ninguna obligación al respecto propiamente dicha sino, por el contrario, una serie de derechos sobre los datos de su titularidad. Sin embargo, el hecho de que un tercero trate tales datos es una actividad que sí quedaría vinculada por esta normativa.

En este sentido, la Directiva 95/46/CE define en su artículo 2 b) el concepto de "tratamiento de datos personales" como cualquier operación o conjunto de operaciones, efectuadas o no mediante procedimientos automatizados, y aplicadas a datos personales, como la recogida, registro, organización, conservación, elaboración o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma que facilite el acceso a los mismos, cotejo o interconexión, así como su bloqueo, supresión o destrucción.

Por todo ello, teniendo en cuenta estas consideraciones, podría establecerse que una dirección IP tendría la consideración de dato de carácter personal, en la medida en que es una información numérica que, la entidad o persona que se encuentra tratándola, podría relacionarla, en último término, con un determinado usuario, el cual, en última instancia, sería una persona

física. Por ejemplo, una dirección IP podría ser relacionada con el usuario titular de la misma, por parte de su proveedor de acceso a Internet o por su proveedor de servicios en Internet.

El Grupo del Artículo 29 establece que *"el Considerando 26 de la Directiva 95/46 especifica que los datos son calificados como personales en tanto en cuanto se pueda establecer una conexión con la identidad del sujeto de los datos (en este caso el usuario de la dirección IP), por el responsable del tratamiento o cualquier tercero por medios razonables. En el caso de la dirección IP, el ISP es siempre capaz de establecer una conexión entre la identidad del usuario y la dirección IP y de esta forma, por ejemplo, terceras personas podrían hacer uso de ellas a través de los registros disponibles de direcciones IP establecidas o usando otros medios técnicos existentes".*

La posibilidad de asociación de un dato personal a una persona concreta se favorece, en principio, con IPv6, ya que algunas de las direcciones creadas en base a esta versión 6 del Protocolo, incluirían un identificador de usuario único (Interface ID: 64 bits) que identificaría inequívocamente a cada terminal (PC, ordenador portátil, PDA´s, etc), el cual podría incluso terminar siendo asociado a un determinado usuario a partir de distintos mecanismos (por ejemplo, guías públicas, bases de datos públicas del estilo a la base de datos Whois, etc) que serán tratados posteriormente en este libro.

Por último, es importante resaltar que las implicaciones en materia de protección de datos que podrían existir como consecuencia de la implantación de esta nueva versión del Protocolo no surgen exclusivamente por el hecho de que la dirección IP pueda asociarse a una persona sino porque, incluso, ésta puede actuar a modo de "matrícula" de la persona respecto de los actos que realice. En este sentido, podría existir mucha información originada a partir de dicha IP y asociable a ésta, por ejemplo, compras, comportamientos, datos personales, etc.

2.2.1. ¿En todos los casos las IP basadas en un Identificador Único son datos de carácter personal?

Si bien, en líneas generales, se afirma que las direcciones IP basadas en la nueva versión 6 del Protocolo, que contienen en su configuración un Identificador Único, son datos de carácter personal, es importante resaltar que no siempre es así.

Para que esta afirmación sea cierta, sería necesario poder asociar dicha IP a una determinada persona física, lo cual podría ser posible como se verá en apartados posteriores.

Imaginemos un ordenador personal que se encuentra conectado a la red de Internet utilizando el protocolo IPv6. En este sentido, el usuario, a través de su terminal, accedería a la Red a través de una dirección IP única cuyo Identificador Único, que forma parte de ella, estaría identificando a su terminal de forma directa y al usuario titular, de forma indirecta.

En este caso y dando por supuesto que el proveedor de servicios en Internet tuviera la posibilidad de asociar la dirección IP al usuario, titular de la misma, por ejemplo, como

consecuencia de la contratación de servicios efectuada con este usuario, para el proveedor, la dirección IP del usuario sería claramente un dato de carácter personal.

Por el contrario, imaginemos este mismo supuesto, pero en el cual dicho ordenador personal pertenece a un Cibercafé, de manera que el usuario que accede a través de dicha dirección IP variaría cada cierto espacio de tiempo.

En este segundo supuesto, probablemente, el proveedor de servicios de Internet no podría asociar dicha dirección IP a un usuario concreto, por lo que el dato de dirección IP no tendría una consideración clara como dato personal.

2.2.2. ¿Son las direcciones IP basadas en un Identificador Único correspondientes al lugar de trabajo, datos de carácter personal?

Se han planteado dudas acerca de si una dirección IP que identifica un determinado puesto de trabajo (dispositivo, ordenador) en una compañía, podría tener la consideración de un dato personal, habida cuenta de que, en líneas generales, las actividades desarrolladas a través de la misma, no estarían incluidas en el ámbito íntimo del usuario que la utiliza.

En concreto, es frecuente que se piense que una dirección IP de carácter particular es un dato personal y, en cambio, la IP de un puesto de trabajo no lo es, por no pertenecer a la esfera íntima del usuario.

En principio, podría considerarse que esta valoración no es acertada desde el punto de vista de la normativa de protección de datos ya que, el único criterio a tener en cuenta para determinar si una dirección IP es un dato personal, es que dicha dirección IP pueda relacionarse con la persona física que dirige el nodo o el terminal que está accediendo a la Red.

En cuanto a las posibilidades de relacionar dicha dirección IP con una persona física concreta, será necesario tener en cuenta las consideraciones que sobre este aspecto, se recogen en apartados posteriores de este libro ya que, ciertos proveedores (en adelante, agentes tratantes o actores) podrán realizar esta asociación de una forma directa, mientras que otros no tendrán esta posibilidad o tendrán que acudir a medios alternativos de asociación.

3. Normativa de Protección de Datos

El objeto de este apartado es realizar un breve análisis de las Directivas y Convenios europeos más importantes en materia de protección de datos, los cuales podrían ser de aplicación, inicialmente, al Protocolo IPv6.

Sin embargo, no corresponde ser objeto del mismo, el análisis de la progresión de las distintas normativas existentes sobre esta materia ni el estudio sobre el inicio de la preocupación acerca de la protección de datos personales en los distintos Estados, habida cuenta de que este asunto ya ha sido tratado en el Capítulo II.

Protección de datos personales

En este sentido, el objetivo principal de los siguientes capítulos es de naturaleza triple:

- Conocer cómo se encuentra regulado, actualmente, el tratamiento de datos de carácter personal en Europa, a través del análisis de los bloques normativos principales.
- Conocer cómo los Estados Miembros han incluido en sus ordenamientos jurídicos estas obligaciones, resaltando aquellas particularidades más importantes localizadas en todas ellas.
- Discernir si IPv6 quedaría perfectamente regularizado a través de la normativa vigente en esta materia o si, por el contrario, existen otras particularidades que, necesariamente, deberán ser tenidas en cuenta por la legislación.

3.1. Convenio de 28 de enero de 1981, del Consejo de Europa, para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal.

Este Convenio, también denominado Convenio 108, es la representación de uno de los primeros esfuerzos efectuados a nivel internacional para la creación y divulgación de las normativas establecidas en materia de protección de datos, tendentes a regularizar los tratamientos de los datos personales de las personas físicas.

A través del mismo, los Estados firmantes adquirieron el compromiso de tomar *"en su derecho interno, las medidas necesarias para que sean efectivos los principios básicos para la protección de datos ..."*.

Precisamente, el objetivo de este Convenio es *"garantizar, en el territorio de cada Parte, a cualquier persona física sean cual fueren su nacionalidad o su residencia, el respeto de sus derechos y libertades fundamentales, concretamente su derecho a la vida privada, con respecto al tratamiento automatizado de los datos de carácter personal correspondientes a dicha persona"*.

3.2. Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos

Transcurridos bastantes años desde la firma del Convenio 108, surge en 1995 la Directiva 95/46/CE, a través de la cual se aportan a los Estados Miembros los principios en materia de protección de datos que deben regir sus ordenamientos jurídicos nacionales. De esta

manera, se crea un marco legislativo común y homogéneo a nivel comunitario aplicable a los Estados Miembros.

Tal y como se desprende de su Considerando 25, su objeto es garantizar la protección de los datos personales que vayan a ser tratados tanto por entidades públicas como privadas, de forma automatizada. En concreto, establece que "*las personas, autoridades públicas, empresas, agencias u otros organismos que realicen tratamientos de datos personales tienen las obligaciones impuestas en esta Directiva, en particular, a la calidad de los datos, la seguridad técnica, la notificación a las autoridades de control y el resto de obligaciones que incumben a la realización de tratamientos legítimos y, por último, el respeto a los derechos de los titulares de los datos*".

3.3. Directiva 97/66 del Parlamento Europeo y del Consejo, de 15 de diciembre, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las telecomunicaciones

Teniendo en cuenta la gran proliferación de nuevas redes digitales públicas avanzadas de telecomunicaciones y los importantes tratamientos de datos personales efectuados por las operadoras de telecomunicaciones, se publicó esta Directiva, a través de la cual se definían los principios que deberían regir los tratamientos específicos de datos llevados a cabo en los servicios de telecomunicaciones.

En concreto, alguno de estos aspectos son:

- El tratamiento de datos de tráfico y facturación
- La facturación desglosada
- La presentación y limitación de la identificación de la línea llamante y conectada
- Las guías públicas con datos personales de los abonados, etc.

Como puede observarse, lejos de establecerse un marco general como ocurre con la Directiva 95/46/CE, la Directiva 97/66 entraba a solucionar problemas concretos de este sector, los cuales, en numerosas ocasiones, podrían servir como referente a la hora de resolver posibles problemáticas detectadas a nivel IPv6, como por ejemplo, la regulación ofrecida respecto de la limitación de la línea llamante o respecto de las guías públicas de abonados.

Sin embargo, esta Directiva se ha visto derogada por la reciente Directiva 2002/58. No obstante, si bien ésta última amplía su regulación a todo el marco de la protección de datos en relación con las nuevas tecnologías (telecomunicaciones y comunicaciones electrónicas, en general), mantiene parte de la regulación ya establecida en la Directiva 97/66.

Protección de datos personales

3.4. Directiva 2002/58/CE del Parlamento Europeo y del Consejo, de 12 de julio, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas

Tal y como se determinaba anteriormente, esta Directiva procedió a la derogación de la Directiva 97/66 y a través de la misma se pretende especificar y completar las disposiciones de la Directiva 95/46/CE para un sector concreto, el de las comunicaciones electrónicas.

Con esta norma se pretende proteger y custodiar la intimidad de los abonados y usuarios de servicios de comunicaciones electrónicas. En concreto, esta Directiva regula, principalmente, los siguientes aspectos:

- La seguridad técnica y de gestión que deben adoptar los proveedores de servicios de comunicaciones electrónicas
- La confidencialidad de las comunicaciones
- El tratamiento de datos de tráfico
- La facturación desglosada
- La presentación y restricción de la línea de origen y la conectada
- El tratamiento de los datos de localización
- Las guías de abonados, etc.

3.5. Desarrollos legislativos en los distintos Estados Miembros

Como consecuencia del Considerando 22 y del artículo 32 de la Directiva 95/46/CE, los Estados Miembros quedaron obligados a adecuar su legislación a las consideraciones efectuadas por esta Directiva, relativa a las condiciones generales de licitud en el tratamiento de datos personales. Por este motivo, los distintos Estados comunitarios han ido adoptando sus propias normativas nacionales tendentes a regular estos aspectos.

Algunas de estas legislaciones nacionales serán analizadas en el siguiente apartado de este libro.

4. Normativa de protección de datos vigente en relación con el uso del Protocolo IPv6

Es objeto de este apartado conocer el grado de adecuación de las Directivas anteriormente citadas y analizadas en el Capítulo II de este libro, a la implantación del Protocolo IPv6,

a los efectos de poder determinar si las mismas prevén todos aquellos aspectos nuevos que pudieran surgir como consecuencia de esta implantación o si, por el contrario, deberían verse modificadas.

En especial, el análisis se centrará en la Directiva 95/46/CE, como consecuencia de su consideración como el principal bloque normativo en protección de datos, delimitadora de los criterios básicos a tener en cuenta por las regulaciones de los distintos Estados Miembros. Asimismo, será efectuado este análisis respecto de la Directiva 2002/58/CE como consecuencia de su mayor adaptación al mundo de las comunicaciones electrónicas, dentro del cual podrían ubicarse las funcionalidades del nuevo Protocolo en su versión 6.

Para finalizar, se recogerán unas breves consideraciones acerca de la adecuación de alguna de las normativas nacionales adoptadas por los Estados Miembros en relación con esta materia.

4.1. Directiva 95/46/CE

A efectos aclarativos, el análisis de esta Directiva se centrará en tres aspectos fundamentales existentes en el tratamiento de los datos personales y, en concreto, en el tratamiento del dato de dirección IP.

En concreto, estos momentos principales son:

- La obtención del dato de dirección IP
- El tratamiento del dato de dirección IP por los agentes tratantes cuando éstos son capaces de asociar dicho dato a un terminal e incluso a un usuario
- La cancelación y supresión del dato de dirección IP

A lo largo de cada uno de estos momentos principales, normalmente existentes en cualquier tratamiento de datos, la normativa sobre esta materia prevé una serie de principios y obligaciones que cualquier agente tratante deberá tener en cuenta. Pues bien, en este apartado, se analizará si respecto del tratamiento del dato de dirección IP conforme a estos momentos clave (recogida, tratamiento y cancelación), las disposiciones de la Directiva prevén la regulación apropiada para la nueva versión 6 de este Protocolo.

4.1.1. La obtención del dato de dirección IP

Tres son las principales obligaciones impuestas por esta normativa que deberán ser tenidas en cuenta cuando se proceda a recabar datos de carácter personal por cualquier persona, tanto física como jurídica: calidad de los datos; deber de información y obtención del debido consentimiento.

Protección de datos personales

A) Respecto del **principio de calidad de los datos**, el artículo 6 exige que los datos recabados sean:

- Tratados de forma leal y lícita
- Recogidos para fines determinados, explícitos y legítimos
- No sean tratados, posteriormente, para fines no compatibles
- Adecuados, pertinentes y no excesivos respecto de los fines que motiven su obtención
- Exactos y actualizados
- Conservados en una forma que permita identificar a su titular por un periodo no superior al necesario.

Las consecuencias derivadas de este artículo para IPv6 supone que tanto el tratamiento del dato de dirección IP, considerado como un dato personal en sí mismo, como el de los datos que puedan ser asociados a una IP, deben regirse por estos parámetros.

B) Respecto del **deber de información**, el artículo 10 establece los puntos respecto de los cuales, la persona física o jurídica que recaba los datos, deberá informar a los titulares de los mismos:

- Identidad del responsable del tratamiento y, en su caso, de su representante
- Fines del tratamiento
- Destinatarios de los datos
- Carácter obligatorio de la aportación de los datos
- Ejercicio de los derechos de acceso y rectificación

En consecuencia, en el momento en el que se obtenga tanto el dato de la dirección IP como los datos que potencialmente puedan asociarse a ésta, deberá ser informado el interesado de estos aspectos.

El principal problema es que este artículo es aplicable cuando el usuario aporta sus datos a la entidad que corresponda pero se plantea el supuesto de que, en ocasiones, el usuario estará aportando su dirección IP con su mera conexión y navegación por la Red y, por lo tanto, sin ser plenamente consciente de dicha aportación. En este caso, se plantea quiénes están obligados a dar cumplimiento a esta obligación y el modo de hacerlo.

Si bien, la contestación a este problema debe analizarse caso por caso, una contestación genérica supondría que toda persona física o jurídica que con motivo de la conexión y/o navegación por la Red de un usuario, conozca su IP, la trate, la almacene y pueda asociarla

a la persona física titular, estará obligado por esta disposición, así como por el resto de los requerimientos de la Directiva.

Por otro lado, el artículo 11 hace referencia a los supuestos en los que se debe informar aunque los datos no se hubieran obtenido directamente de los usuarios, por ejemplo, a través de la obtención del dato de dirección IP y de la información asociada a la misma, facilitada por un proveedor de acceso a Internet a una empresa de marketing, dedicada al estudio de perfiles de usuarios.

Como puede observarse, estos artículos establecen obligaciones que, en ciertos casos, pueden conllevar ciertas dificultades prácticas para su adopción por cada uno de los agentes tratantes. En este sentido, como será analizado en el apartado 5.6 de este Capítulo, una dirección IP sería, en principio, asociable a su titular por parte de un proveedor de acceso a Internet. Sin embargo, podrían existir otra serie de agentes tratantes (i.e un prestador de servicios de tienda virtual) que a través de medios razonables (guías públicas, bases de datos, etc) tuvieran la posibilidad de asociar la IP con su titular. En estos casos, se plantea la duda de decidir quién deberá proceder al cumplimiento de este deber de información: el proveedor de acceso; el proveedor de los servicios de tienda virtual o ambos.

C) Por último, respecto de la **obtención del consentimiento** para el tratamiento de la dirección IP y de la información que pudiera asociarse a la misma, el artículo 7 de la Directiva establece que sólo podrán tratarse los datos cuando:

- El interesado consienta (expresamente, en unos casos y tácitamente, en otros)
- El tratamiento sea necesario para la ejecución de un contrato en el que el interesado sea parte
- Sea necesario para cumplir una obligación jurídica
- Sea necesario para proteger el interés vital del interesado
- Sea necesario para satisfacer un interés legítimo del responsable del tratamiento o de aquellos a los que se le comuniquen los datos.

En definitiva, el tratamiento del dato de dirección IP deberá llevarse a cabo siempre que el titular consienta o bien, cuando se den alguna de las circunstancias apuntadas anteriormente, las cuales podrán ser completadas en las distintas normativas nacionales adoptadas por los Estados Miembros.

Asimismo, la Directiva, en su artículo 8, establece una serie de requisitos mayores para cuando los datos tratados (en el supuesto analizado, los datos asociados a una dirección IP determinada) pertenezcan a categorías especiales (origen racial o étnico, opiniones políticas, convicciones religiosas o filosóficas, afiliación sindical, salud o sexualidad).

Protección de datos personales

En este sentido, la Directiva prohíbe el tratamiento de estos datos a no ser que éste se encuentre fundado en alguna de las excepciones que se establecen como, por ejemplo, la obtención del consentimiento explícito del titular de los datos, el tratamiento con el fin de salvaguardar el interés vital del tercero, o con fines de diagnóstico médico, prestación sanitaria, etc.

Estas puntualizaciones son relevantes desde el punto de vista de determinados supuestos en los que un proveedor de servicios pueda tener acceso a este tipo de datos. Por ejemplo, imaginemos un proveedor de contenidos eróticos que dispone de una página web a la que pueden acceder los usuarios. Si alguno de ellos accediera con una IP basada en un Identificador Único, éste podría tener información acerca del tipo de contenidos de orientación sexual al que éste accedería y, además, asociarla al terminal y potencialmente al usuario.

En este sentido, estaría tratando datos de sexualidad asociados a una IP y a un usuario, con lo que dicho tratamiento quedaría vinculado por las disposiciones contenidas en este artículo.

4.1.2. El tratamiento del dato de dirección IP

Una vez recabados los datos (la dirección IP en sí misma y, en algunos casos, otra información personal que pudiera asociarse a ésta), la Directiva prevé otra serie de artículos tendentes a regularizar el tratamiento que se efectúe sobre los mismos.

A través de estos artículos, se establece la obligación de adoptar por los agentes tratantes, una serie de medidas tanto técnicas como organizativas para asegurar la confidencialidad, integridad y seguridad de los datos. La Directiva no establece el tipo de medidas a implantar, por lo que deja que las distintas legislaciones nacionales las determinen.

Asimismo, establece cómo debe llevarse a cabo el tratamiento de los datos por terceros distintos de la persona física o jurídica responsable de los mismos.

4.1.3. La cancelación o conservación del dato de dirección IP

La Directiva no se pronuncia de forma clara acerca de los parámetros que deben tenerse en cuenta para proceder a la cancelación o a la conservación de los datos personales. Por lo tanto, a través de la Directiva no es posible conocer por cuánto tiempo deberán conservarse las direcciones IP en los sistemas de los agentes tratantes o en qué supuestos deberán cancelarse.

Al igual que ocurre para el resto de los datos personales, habrá que estar a lo dispuesto en las legislaciones nacionales de los Estados Miembros para poder determinar con cierta exactitud los citados plazos de conservación, atendiendo en su caso, al resto de normativa que fuere aplicable a cada supuesto de conservación de datos.

4.1.4. ¿Debe modificarse la Directiva 95/46/CE con la implantación del Protocolo IPv6?

Es indiscutible que uno de los principales debates generados como consecuencia de la futura utilización del nuevo Protocolo, se cierne en conocer si resultaría necesaria o no la modificación

de esta Directiva a los efectos de adaptarla a nuevos problemas que pudieran ocasionarse como consecuencia de este Protocolo o si, por el contrario, a través de la misma se regulan los aspectos fundamentales aplicables al mismo.

Tal y como se ha determinado, los artículos de la Directiva podrían considerarse, en principio, aplicables a los tratamientos de datos derivados del uso del protocolo IPv6 y, por lo tanto, puesto que las consecuencias derivadas de éste no discrepan o contradicen los principios, obligaciones y derechos estipulados en la Directiva 95/46/CE y, tomando como apoyo lo establecido por ésta misma a través de su Considerando 68, cabría determinar que, en principio, no resultaría necesaria la modificación de la citada Directiva.

A efectos aclaratorios, el citado Considerando establece lo siguiente: *"Considerando que los principios de protección de los derechos y libertades de las personas y, en particular, el respeto de la intimidad en lo que se refiere al tratamiento de los datos personales objeto de la presente Directiva podrán completarse o precisarse, sobre todo en determinados sectores, mediante normas específicas conformes a estos principios".*

Asimismo, la labor de adecuación de estos principios a sectores más específicos deberá efectuarse, por ejemplo, a través de normas de desarrollo y de códigos tipo que facilitan que, de una manera dinámica y flexible, se adapten las consideraciones relativas al tratamiento de datos personales a cada sector.

El propio artículo 27 de la Directiva diferencia entre Códigos de Conducta de ámbito nacional, los cuales deberán ser potenciados por los Estados Miembros y revisados por las Autoridades nacionales y los Códigos de ámbito comunitario, los cuales serán sometidos a la revisión del Grupo del Artículo 29.

4.2. Directiva 2002/58/CE

Esta Directiva se corresponde con la regulación comunitaria en materia de protección de datos que más se ajusta al supuesto que es objeto de análisis en este libro, ya que a través de la misma se pretenden tratar las necesidades específicas en materia de protección de datos respecto de los nuevos servicios de comunicaciones electrónicas de la sociedad de la información. Algunos de los aspectos regulados podrían ser los servicios de localización de terminales, el suministro de información, el tratamiento de los datos de tráfico relativos a las comunicaciones llevadas a cabo y, en general, cualquier servicio que pudiera ser prestado a través de redes públicas de comunicaciones electrónicas.

Asimismo, es importante resaltar que en todo aquello que no sea tratado por esta Directiva será de aplicación la Directiva 95/46/CE. Por este motivo, en este apartado sólo se tratarán las particularidades recogidas en esta Directiva 2002/58/CE.

Protección de datos personales

4.2.1. Consideración del dato de dirección IP como un dato de tráfico

Uno de los conceptos más relevantes desde el punto de vista del Protocolo IPv6, tratados por esta Directiva es el concepto de "Datos de tráfico" el cual se encuentra definido en el apartado b) del artículo 2 de la citada Directiva.

En concreto, debe entenderse por dato de tráfico, *"cualquier dato tratado a efectos de la conducción de una comunicación a través de una red de comunicaciones electrónicas o a efectos de la facturación de la misma".*

Por "comunicación" debe entenderse *"cualquier información intercambiada o conducida entre un número finito de interesados por medio de un servicio de comunicaciones electrónicas".*

En este sentido, el propio Considerando 15 de la misma aclara que *"los datos de tráfico pueden referirse, entre otras cosas, al encaminamiento, la duración, la hora o el volumen de una comunicación, al protocolo utilizado, a la localización del equipo terminal del remitente o destinatario, a la red en que se origina o concluye la transmisión, al principio, fin o duración de una conexión".*

En consecuencia, es posible considerar que el dato de dirección IP puede ser considerado como un dato de tráfico en la medida en la que éste posibilita la conducción de las comunicaciones a través de redes de comunicaciones electrónicas.

En este sentido, la Directiva introduce una serie de parámetros dedicados a la forma de tratar este tipo de datos.

4.2.1.1. Consideraciones generales relativas a los datos de tráfico

Uno de los principales puntos relativos a los datos de tráfico recogidos en el artículo 5 de la Directiva es el relativo a la exigencia de garantizar la confidencialidad, no sólo de la información transmitida sino también de los datos de tráfico relacionados con ésta.

Únicamente podrán ser interceptadas, grabadas, almacenadas, escuchadas o vigiladas estas comunicaciones y los datos de tráfico asociados a las mismas cuando:

- El usuario haya consentido
- Las personas que desarrollan estas actuaciones estén autorizadas legalmente

Sin embargo, como es lógico, la Directiva permite el almacenamiento técnico de la información y de los datos de tráfico, necesario para la conducción de la información. Por ello, el almacenamiento que puedan realizar los proveedores de acceso a Internet, operadores de telecomunicaciones, etc, siempre que se realice con esta única finalidad, estaría permitido por la Directiva.

Extrapolando estas consideraciones a IPv6, las direcciones IP, como datos de tráfico, deben ser confidenciales. El cumplimiento de esta obligación es más importante respecto de las IP generadas con un Identificador Único puesto que sería más sencillo asociar por terceros no autorizados, el contenido de la comunicación, con la IP, con el terminal y con el usuario que la genera.

Por este motivo, y siguiendo con lo establecido por este artículo, se podrán tratar estos datos para la conducción de las comunicaciones, para la facturación de los servicios y como prueba de una transacción comercial por las entidades destinadas a la prestación de los mismos. Para cualquier otro tratamiento de este tipo de datos (por ejemplo, promoción comercial o prestación de servicios de valor añadido), en principio y como regla general, se requerirá el consentimiento del titular.

Por último, destacar que los agentes tratantes de estos datos, en todo caso, deberán dar cumplimiento a los parámetros del deber de información y obtención del debido consentimiento, conforme se ha reflejado en el apartado anterior.

4.2.1.2. ¿Cuál es el periodo de conservación de los datos de tráfico?

La Directiva permite almacenar los datos de tráfico por determinados proveedores, pero conforme a una serie de criterios que garanticen que dicho almacenamiento se efectúa por el tiempo necesario. En concreto, deben eliminarse cuando hayan dejado de ser necesarios para la transmisión de la comunicación. No obstante, permite su tratamiento a efectos de facturación del servicio y pagos de interconexiones, por lo que deberá deducirse que los datos de tráfico deberán eliminarse cuando no sean necesarios para el cumplimiento de estas finalidades.

El Considerando 27 aclara el término "dejar de ser necesarios para la transmisión" cuando determina que, por ejemplo, *"para una llamada de telefonía vocal, la transmisión finalizará en cuanto uno de los usuarios interrumpa la conexión; para el correo electrónico la transmisión finaliza en cuanto el destinatario recoge el mensaje, en general, del servidor de su proveedor de servicios"*.

Asimismo, es significativo que una de las alternativas que ofrece la Directiva a la eliminación de estos datos de tráfico es "hacerlos anónimos" lo cual plantea ciertas dificultades prácticas para los proveedores de servicios, en el caso de IP generadas por Identificador Único. Este hecho requeriría adoptar algún tipo de medida que les impida asociar la IP con el usuario contratante, titular de la misma.

Si bien, estas son las consideraciones de la Directiva, es importante poner de manifiesto una nueva tendencia legislativa que se está forjando en la UE, en las fechas de elaboración de este libro, derivada, entre otros motivos, en la necesidad de luchar y perseguir los delitos

de terrorismo, la cual conlleva una serie de modificaciones respecto del tratamiento y conservación de los datos de tráfico.

En concreto, a través de la nota de prensa 7555/04 (Presse 94) de la Sesión Extraordinaria del Consejo de Justicia y Asuntos de Interior, celebrada en Bruselas el 19 de marzo de 2004 como consecuencia de los atentados terroristas perpetrados en Madrid y presidida por D. Michael McDowell, ha sido manifestada la intención de la Comisión Europea de presentar en el mes de junio, una propuesta legislativa para obligar a los operadores de Internet y a los operadores telefónicos a conservar, (aproximadamente durante un periodo mínimo de 2 a 3 años), los datos de tráfico de los usuarios, con el objetivo principal de combatir el uso de Internet como medio canalizador de la comisión de actos terroristas.

Esta futura regulación no sería contradictoria con lo establecido por la presente Directiva ya que en su artículo 15 se permite la limitación de los derechos de los usuarios y abonados en aras de proteger la seguridad, investigación y descubrimiento de la comisión de actos delictivos y conservarlos por más tiempo en base a estos motivos.

Sin embargo, sería necesario regular las limitaciones al uso de esta información durante el tiempo en el que esté permitida su conservación.

4.2.2. ¿Cuándo requiere la Directiva que se obtenga el consentimiento de los usuarios / abonados para el tratamiento de sus datos?

En líneas generales, el espíritu de la Directiva pretende que cualquier actividad relacionada con el suministro de servicios de comunicaciones electrónicas que vayan más allá de la transmisión de una comunicación o de su facturación (i.e. la prestación de servicios de valor añadido), deberá basarse en datos anónimos y, en el caso de que esto no fuera posible, obtener el consentimiento de los titulares.

4.2.3. Restricción de la identificación de la línea de origen

Otro de los principales artículos que podría ser aplicable por analogía a IPv6 es el artículo 8 dedicado a la presentación y restricción de la línea de origen y de la línea conectada. En este sentido, si bien este artículo podría parecer más destinado a la regulación de los servicios de telefonía (móvil o fija), en principio, podría entenderse como aplicable para el supuesto de comunicaciones electrónicas efectuadas a través del Protocolo IPv6.

A través del mismo se manifiesta la voluntad del legislador de preservar la intimidad del usuario que efectúa la llamada, obligando a los proveedores del servicio a ofrecerle la posibilidad técnica de que evite la identificación de la línea llamante, cuando exista la posibilidad de que ésta pueda ser visualizada.

Asimismo, desea proteger los intereses del usuario que recibe las llamadas permitiéndole excluir la recepción de llamadas por parte de usuarios que hubieran impedido la identificación de su línea llamante.

Siguiendo el criterio establecido en este artículo, podría determinarse que respecto de las direcciones IP formalizadas en base de un Identificador Único, podría exigírsele a los proveedores la posibilidad de adoptar ciertos mecanismos que impidan:

- La identificación de la dirección IP del usuario en las comunicaciones que efectúe, siempre que esta identificación no fuera necesaria.
- La posibilidad de evitar la recepción de comunicaciones transmitidas a través de una determinada IP, cuando el usuario que origina la llamada haya evitado el conocimiento de su IP.

No obstante, el Considerando 19 establece que en los casos particulares en los que la adopción de estas medidas sea técnicamente imposible para el proveedor o en los que se requiera un esfuerzo económico desproporcionado, la implantación de estas medidas no tendrá carácter obligatorio. En todo caso, los usuarios deberán ser informados de esta imposibilidad y los Estados Miembros, notificarlo a la Comisión.

En cierto modo, en la actualidad, se están adoptando ciertas medidas técnicas encargadas de favorecer este tipo de actividades que, por analogía, parece que deberían ser aplicables respecto de las direcciones IP, algunas de ellas basadas en el estándar RFC3041.

No obstante, la Directiva enumera varios casos en los que el servicio de anulación de la identificación de la línea llamante, no deberá ser prestado por los proveedores de servicios de comunicaciones electrónicas:

- Para identificar el número de origen de llamadas malevolentes o molestas
- Para atender llamadas de urgencia por parte de organismos reconocidos por los Estados Miembros para prestar estos servicios, policía, ambulancias, bomberos, etc.

4.2.4. Consideración del dato de dirección IP como dato de localización

Por "dato de localización" debe entenderse, conforme establece el apartado c) del artículo 2 de la Directiva *"cualquier dato tratado en una red de comunicaciones electrónicas que indique la posición geográfica del equipo terminal del usuario de un servicio de comunicaciones electrónicas disponible para el público."*

Conforme al Considerando 14, los datos de localización serán aquellos referidos a *"la latitud, longitud y a la altitud del equipo terminal del usuario, a la dirección de la marcha, al nivel*

de precisión de la información de localización, a la identificación de la célula de red en la que está localizado el equipo terminal en un determinado momento o a la hora en que la información de localización ha sido registrada".

En la redes móviles digitales es posible que se traten los datos sobre localización (los cuales son considerados datos de tráfico) que pueden proporcionar la posición geográfica del equipo terminal móvil del usuario para hacer posible la transmisión de las comunicaciones.

Este hecho adquiere mayor relevancia en los supuestos en los que un dispositivo con movilidad (PDA´s, portátiles, teléfonos móviles, etc) acceda a la Red a través de una IP, puesto que además de existir la posibilidad de rastrear su navegación, sería posible conocer su ubicación física, tanto del terminal como del propio usuario titular del mismo.

Esta posibilidad abre numerosos frentes de tratamientos de datos que deberán regularizarse conforme a la Directiva 95/46/CE y a las legislaciones nacionales de desarrollo de la misma, por ejemplo, la posibilidad de adquirir (en la mayor parte de los casos de forma ilícita) este tipo de información por prestadores de servicios de información sobre las condiciones del tráfico por carretera para ofrecer determinados servicios a un usuario, en ocasiones sin que éste los hubiera solicitado (por ejemplo, estado del tráfico en la carretera por la que circula); el control de los teletrabajadores o la creación de perfiles, hábitos de viaje de una determinada persona, lo cual, desde un aspecto meramente comercial, podría reportar importantes ventajas económicas para aquellos agentes que deseen aprovecharse de este tipo de avances tecnológicos.

En este sentido, es fundamental resaltar que la Directiva establece que este tipo de datos, únicamente, podrán tratarse con el consentimiento informado del usuario afectado e incluso, aunque éste lo hubiera prestado en un momento determinado, deben establecerse mecanismos que favorezcan la revocación de este consentimiento en cualquier momento.

Asimismo, la Directiva permite que únicamente traten estos datos aquellos agentes que actúen en nombre y por cuenta del proveedor de servicios de comunicaciones electrónicas adquiridos por el usuario, impidiendo su tratamiento por terceros ajenos a éstos.

4.2.5. Regulación de las guías de abonados

Tal y como se verá en apartados posteriores, uno de los medios que permitirían la asociación de una determinada IP con un determinado usuario y, por lo tanto, que potenciaría la consideración del dato de dirección IP como un dato personal, es la adopción de guías públicas que contengan una relación de usuarios con sus respectivas direcciones IP.

Teniendo en cuenta esto, podría servir como criterio a la hora de adoptar esta práctica, lo establecido en esta Directiva, en relación con las guías de abonados.

A través de las mismas, el usuario puede decidir si desea hacer públicos sus datos a terceros o no, pero, en todo caso, la inclusión de los mismos en las citadas guías requerirá que las entidades gestoras o suministradores de las mismas, informen a los titulares de los datos de las finalidades de estas guías, así como del resto de los parámetros del deber de información (cesiones de datos, posibilidad de ejercitar los derechos de acceso, rectificación, etc), por supuesto, obteniendo para ello su consentimiento.

En este sentido, cualquier utilización de estas guías por parte de un agente tratante con fines distintos de aquellos para los que se obtuvo el consentimiento inicialmente del usuario, requerirá que este agente tratante lo obtenga de nuevo.

En resumen, el artículo 12 establece una serie de parámetros que deberán ser tenidos en cuenta por los Estados Miembros a la hora de crear guías públicas:

- Obligación de informar a los titulares de los datos de su inclusión en la guía
- Posibilidad de que las guías sean impresas o electrónicas
- Facultad de decidir por parte de los titulares de los datos, cuáles de ellos van a figurar en las guías
- Respeto al principio de calidad de datos: inclusión de datos adecuados, pertinentes y no excesivos
- Carácter gratuito de la no inclusión, comprobación, corrección o supresión de datos en una guía pública.

El análisis de las consecuencias que la creación de este tipo de guías respecto de las direcciones IP pudiera tener, será llevado a cabo en el apartado 5.3.1. de este Capítulo.

4.2.6. ¿Debe modificarse la Directiva 2002/58/CE con la implantación del Protocolo IPv6?

Actualmente, esta Directiva se corresponde con el marco regulador en materia de protección de la intimidad y de protección de datos personales que más se aproxima a la regulación que debería ser ofrecida para la utilización del nuevo Protocolo IPv6.

La mayor parte de los artículos recogidos en la misma regulan supuestos que, bien directamente o bien de forma más indirecta, se encuentran relacionados con IPv6. En algunos supuestos, como ocurre con la regulación de la posibilidad de restringir la identificación de la línea de origen o la regulación de las guías de abonados, si bien parecería claro que dichos artículos pretenden regular un supuesto de hecho diferente, podrían ser aplicables de forma analógica a la utilización del Protocolo en su nueva versión 6.

Por ello, cabría afirmar que a través de la misma se ofrecen los criterios generales a tener en cuenta, los cuales deberán ser adaptados por los Estados Miembros a la hora de regular,

a través de cada una de sus legislaciones nacionales, el uso de IPv6 y la forma de dar cumplimiento a las obligaciones impuestas tanto en esta Directiva como en la Directiva 95/46/CE.

4.3. Desarrollo normativo en materia de protección de datos de los Estados Miembros

Como consecuencia del Considerando 22 y del artículo 32 de la Directiva 95/46/CE, los Estados Miembros tendrán que adecuar su legislación a las consideraciones efectuadas por la misma. Por este motivo, los distintos Estados comunitarios han ido adoptando sus propias normativas nacionales tendentes a regular estos aspectos.

A efectos meramente informativos, algunos de estos Estados que ya disponen de una normativa, más o menos restrictiva en materia de tratamiento de datos personales son Alemania, Austria, Bélgica, Dinamarca, España, Finlandia, Francia, Gran Bretaña, Grecia, Holanda, Irlanda, Italia, Luxemburgo, Portugal y Suecia.

Tal y como podrá comprobarse, son pocas las innovaciones recogidas en estas normas, las cuales suelen ser un mero reflejo de las disposiciones de la Directiva 95/46/CE de referencia.

4.3.1. Alemania

Alemania fue un país pionero en la adopción de normas de protección de datos, ya que la primera fue la conocida como Ley de Hesse, de 7 de octubre de 1970.

Seguidamente, fue aprobada la Ley Alemana Federal de Protección de Datos, de fecha 27 de enero de 1977, la cual fue modificada por la ley llamada Bundesdatenschutzgesetz (BDSG), la cual entró en vigor el 1 de junio de 1991.

Actualmente la norma que se encuentra en vigor es denominada "The Federal Data Protection Act" (Bundesdatenschutzgesetz) de 18 de mayo de 2001.

Asimismo, es importante destacar que existen numerosas normas adoptadas por distintas ciudades alemanas (Berlín, Brandenburgo, Essen, Saarland, etc) sobre esta materia.

4.3.1.1. Consideraciones a destacar

El propósito de la Norma es proteger el derecho a la privacidad de los individuos frente a los tratamientos de sus datos personales realizados en su perjuicio (artículo 1). Con este fin, la norma es un reflejo fiel del modelo de protección de datos personales creado por la Directiva 95/46/CE y regula principios y obligaciones como los requisitos de calidad en la obtención de los datos; necesidad de obtención del consentimiento para el tratamiento; principio de seguridad y auditoría, etc.

Es relevante, dentro del texto de la Norma, que la persona que provee un medio de grabación o procesamiento de datos personales, que instala dicho medio o que modifica o pone a disposición un procedimiento para el procesamiento automático de datos personales que funcione total o parcialmente en un medio como el citado, debe informar al interesado de ciertos aspectos, a menos que éste tuviera conocimiento de los mismos (artículo 6 c).

Asimismo, en su Capítulo III, se regula el funcionamiento de la Autoridad de Control alemana (Federal Data Protection Commissioner).

4.3.2. Austria

La primera ley austriaca de protección de datos (Datenschutzgesetz) data del 18 de octubre de 1978 y fue posteriormente modificada por la decisión 609/1989 de la Corte Constitucional.

Actualmente, la norma que se encuentra en vigor es el Federal Act Concerning the Protection of Personal Data (Dasenschutzgesetz 2000), la cual entró en vigor el 1 de enero del año 2000.

Asimismo, distintas regiones (Länders) han adoptado su normativa a esta ley, tales como Kärnten, Salzburgo o Viena, entre otras.

4.3.2.1. Consideraciones a destacar

Alguno de los aspectos más relevantes tratados por esta Norma son los siguientes:

- El derecho a la protección de datos se considera como un derecho fundamental (artículo 1).
- Las restricciones al deber de confidencialidad solo están permitidas cuando se trate de proteger un interés superior y legítimo de un tercero (artículo 1).
- Los intervinientes en un sistema o conjunto de información (sistema de procesamiento conjunto de datos por varios responsables con acceso recíproco a los datos) deberán señalar un operador cuyo nombre y dirección sea incluido en el Registro de Procesamiento de Datos (artículo 50).

En definitiva, además de cumplir con la necesidad de trasposición de la Directiva 95/46/CE, la ley austriaca regula, sin salirse de la norma comunitaria, algunos supuestos que no aparecen en otros ordenamientos, como el citado del artículo 50.

4.3.3. Bélgica

La primera norma en materia de protección de datos adoptada en Bélgica es de 8 de diciembre de 1992.

Actualmente, la normativa vigente entró en vigor el 1 de septiembre de 2001.

Protección de datos personales

4.3.3.1. Consideraciones a destacar

Se señala que toda persona física tiene derecho a la protección de sus libertades y Derecho fundamentales, particularmente a la protección de la vida privada, en el tratamiento de sus datos de carácter personal (artículo 2).

El ámbito de aplicación de la ley se extiende tanto a los tratamientos automatizados como a los no automatizados (artículo 3). Siguiendo esta línea inicial, la Norma viene a reflejar los requerimientos establecidos por la Directiva 95/46/CE y, por lo tanto, alguno de los principios y obligaciones contenidos en la misma son la obligación de notificar ficheros; el respeto a los derechos del titular de los datos; el especial tratamiento de los datos sensibles, etc.

4.3.4. Dinamarca

En Dinamarca, la primera legislación de protección de datos fue doble: una primera norma aplicable a ficheros de titularidad pública, la Ley 294 de 8 de junio de 1978 sobre registros públicos (posteriormente modificada en varias ocasiones) y una segunda, para ficheros de titularidad privada, la ley 293 de 8 de junio de 1978 sobre registros privados, también modificada en varias ocasiones.

La legislación vigente en esta materia es **"The Act on Processing of Personal Data"** (Act Nº 429) de 31 de mayo del 2000.

4.3.4.1. Consideraciones a destacar

La Norma se aplica a los tratamientos, automatizados o no, de datos personales de personas físicas. No obstante, determinadas partes se aplican, igualmente, a los tratamientos de datos referentes a empresas (artículo 1), con lo que se introduce un cambio significativo en el ámbito de aplicación con relación al que se contiene en la Directiva 95/46/CE.

Como referencia con incidencia en el ámbito de las telecomunicaciones, se indica que no cabrá que las autoridades públicas, empresas privadas, etc. registren de forma automática las llamadas realizadas o recibidas desde sus teléfonos, salvo autorización previa de la autoridad de supervisión y siempre que haya un interés, público o privado, suficiente. Esta prohibición no se aplica cuando se realice por operadores de telecomunicaciones o en la prestación de servicios de identificación de llamada entrante.

4.3.5. España

En el caso de España, la primera norma que entró en vigor fue la conocida LORTAD, Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal.

Posteriormente, esta ley se ha visto derogada por la vigente **Ley Orgánica 15/1999 de 13 de diciembre, de Protección de Datos de Carácter Personal**, también denominada LOPD.

Asimismo, es importante resaltar que como desarrollo del artículo 9 de la LOPD se aprobó el Real Decreto 994/1999 de 11 de junio, por el que se aprueba el Reglamento de Medidas de Seguridad. En este Reglamento se recogen las medidas de seguridad técnicas y organizativas que deberán adoptarse para proteger los ficheros con datos personales que sean tratados por cualquier entidad.

En este sentido, los datos de carácter personal se dividen en tres categorías diferentes (nivel básico, medio y alto) y dependiendo de la categoría de los datos tratados, se adoptarán un tipo de medidas de seguridad u otro.

4.3.5.1. Consideraciones a destacar

La ley tiene por objeto garantizar y proteger, en lo que concierne al tratamiento de los datos personales, las libertades públicas y los derechos fundamentales de las personas físicas y, especialmente, de su honor e intimidad personal y familiar. En términos generales, la norma española es un fiel reflejo del régimen comunitario común establecido por la Directiva 95/46/CE. En este sentido, regula el principio de calidad de los datos; deber de información; necesidad de obtener el consentimiento para el tratamiento (salvo excepciones); especial tratamiento para los datos sensibles; condiciones de tratamiento de datos por terceros, etc.

Alguno de los artículos que podrían estar relacionados con algunos de los temas a tratar en este libro es el relativo a los repertorios telefónicos que son considerados como una fuente accesible al público, en los términos previstos en su normativa específica.

Las fuentes accesibles al público se definen como aquellos ficheros cuya consulta puede ser realizada por cualquier persona, no impedida por una norma limitativa, o sin más exigencia que, en su caso, el abono de una contraprestación (artículo 3). En cuanto a los datos que podrán figurar en las guías de servicios de telecomunicaciones disponibles al público, se remite a sus normas específicas.

4.3.6. Finlandia

La regulación finlandesa en materia de protección de datos personales ha estado basada en tres normas fundamentales:

- Ley de 30 de abril de 1987 sobre ficheros de datos personales
- Ley de 30 de abril de 1987 sobre la Comisión y el Ombudsman de protección de datos
- Decreto de 30 de abril de 1987 sobre ficheros de datos personales

Actualmente, la legislación vigente en esta materia es **"The Finnish Personal Data Act"** (523/1999) de 22 de abril. No obstante, esta ley ha sufrido ciertas modificaciones a partir del **Act on the amendment of the Personal Data Act** (986/2000) que entró en vigor el 1 de diciembre de 2000.

Protección de datos personales

4.3.6.1. Consideraciones a destacar

El artículo 1 de esta Norma establece como su objetivo, implantar en el tratamiento de datos personales, la protección a la vida privada y otros derechos fundamentales que salvaguardan el derecho a la intimidad, así como potenciar el desarrollo de una buena práctica en el tratamiento de datos personales.

Algunas de las reglas generales para el tratamiento de datos personales, enumeradas en el Capítulo 2 de la Norma son: determinación de la finalidad del tratamiento; tratamiento de los datos exclusivamente conforme a dicha finalidad; calidad de los datos; deber de información; tratamiento de datos sensibles, el cual se encuentra prohibido si no median algunas circunstancias tales como la obtención del consentimiento expreso del titular; transferencias internacionales; regulación de los derechos de acceso y rectificación, etc.

Una de las novedades se introduce en la Sección 13 cuando se regula el tratamiento del número personal de identidad, de forma específica, requiriéndose para ello, la obtención del consentimiento inequívoco del interesado.

Asimismo, la Sección 17 regula la creación de registros de consulta pública, de manera que los datos se incluirán en los mismos siempre que su titular no se hubiera negado a ello.

Otra de las novedades se encuentra en la Sección 21 donde se establecen los distintos plazos de conservación de la información por los responsables de los ficheros.

Por último, la Sección 38 crea la autoridad de Control en Finlandia, la cual es denominada "The Data Protection Ombudsman".

4.3.7. Francia

La primera ley francesa sobre esta materia fue la Ley 78-17 de 6 de enero de 1978. Actualmente, se está debatiendo en el Parlamento la adopción de una serie de modificaciones a la misma.

4.3.7.1. Consideraciones a destacar

El tratamiento de datos personales no podrá ser contrario a la identidad humana, los derechos del hombre, la privacidad o las libertades individuales o públicas (artículo 1).

El concepto de tratamiento automatizado de datos se refiere a cualquier serie de operaciones efectuadas por medios automáticos, incluyendo la recogida, la grabación, la preparación, la modificación, el almacenaje y la destrucción de datos personales así como cualesquiera operaciones que se relacionan con el empleo de ficheros o bases de datos, incluyendo interconexiones o comparaciones, la consulta o la comunicación de datos personales (artículo 5).

Puesto que la norma francesa es sensiblemente anterior a la Directiva 95/46/CE, es necesario garantizar su evolución conforme a los criterios marcados por la norma comunitaria y, por lo tanto, estos criterios deberán ser tenidos en cuenta para la nueva normativa que se adopte en Francia.

4.3.8. Gran Bretaña

La legislación británica en materia de protección de datos comienza con la Ley de 12 de julio de 1984 (Data Protection Act), la cual entró en vigor en dos momentos distintos y por partes: 12 de septiembre de 1984 y 11 de noviembre de 1987.

Asimismo, Gran Bretaña dispone de un Reglamento de 13 de octubre de 1985 dedicado al Tribunal de Protección de Datos.

Posteriormente, esta legislación se ha derogado, encontrándose en vigor el **"Data Protection Act" de 1998**

4.3.8.1. Consideraciones a destacar

A través de esta normativa se regulan las distintas obligaciones requeridas por la Directiva 95/46/CE. En la Parte I se recogen algunas de ellas, como el deber de información, obligación de rectificar, bloquear, borrar o destruir los datos de carácter personal o la prohibición de tratar datos personales si previamente no se ha notificado el fichero a la autoridad de control británica denominada "Data Protection Commissioner".

Asimismo, se establece que cualquier tratamiento de datos que se realice con finalidades de prevención o detección de delitos, arresto o enjuiciamiento de los responsables, no estará vinculado por el deber de información. Es decir, el tratamiento del dato de dirección IP y de la información asociada a la misma para estos fines no requerirá informar al titular de la misma.

El principio de obtención del consentimiento como premisa para efectuar un tratamiento o cesión de datos se recoge en la Sección 55.

Por otro lado, The Data Protection Act de 1998 recoge una serie de modificaciones en su cuerpo normativo al Consumer Credit Act del año 1974.

La Parte II recoge la interpretación de los principios enumerados en la norma así como de la determinación de las condiciones a tener en cuenta respecto de estos principios, para el tratamiento de todo tipo de datos y para el tratamiento de datos sensibles, así como una enumeración de los supuestos en los que cada uno de estos principios no son aplicables.

Otro de los aspectos regulados son los procedimientos de inspección o la regulación de las fuentes de acceso público.

Protección de datos personales

4.3.9. Grecia

La Ley de protección de datos griega es la 2472/1997 de protección de las personas con respecto al tratamiento de datos de carácter personal, aprobada el 10 de abril.

4.3.9.1. Consideraciones a destacar

El objeto de esta norma es determinar las condiciones relativas al tratamiento de datos personales y la protección de los derechos humanos, libertades fundamentales y la vida privada, según establece el artículo 1.

De nuevo, siguiendo las consideraciones de la Directiva de referencia (95/46/CE) establece en su articulado el respeto a principios tales como la calidad de los datos, el deber de información, la necesidad de obtener el consentimiento para el tratamiento, salvo las excepciones del artículo 2 y, en todo caso, será necesario el consentimiento escrito para el tratamiento de datos sensibles.

Otros de los temas regulados son la cesión de datos, las cuales deberán ser comunicadas a la Autoridad de control griega y, en el caso de que se basen en datos sensibles, se deberá obtener su autorización; regulación de transferencias internacionales de datos; ejercicio de derechos de acceso y oposición o el régimen de sanciones e infracciones penales y administrativas, entre otras.

4.3.10. Holanda

La primera ley holandesa en materia de protección de datos fue la Ley de 28 de diciembre de 1988, denominada "Wet personenregistraties" y más conocida como WPR.

Actualmente, se encuentra vigente **Personal Data Protection Act de 6 de julio de 2000.**

4.3.10.1. Consideraciones a destacar

Se establece que esta Norma se aplica tanto a los tratamientos automatizados como no automatizados de datos personales.

A través de los artículos 7 al 11 se recogen algunos de los requisitos que deben darse en todo tratamiento de datos: obtención de los datos para fines legítimos y claramente determinados; necesarios para cumplir una obligación legal o el cumplimiento de un contrato (entre otras causas); conservación de los datos por el tiempo necesario para el cumplimiento de la finalidad de tratamiento, etc.

Por otro lado, los artículos 16 al 24 regulan el tratamiento de los datos sensibles (religión, filosofía de vida, política, raza, salud, vida sexual, afiliación sindical; antecedentes criminales).

En algunos casos, por ejemplo, para el tratamiento de datos de raza u origen ético, entre las causas que permiten su tratamiento, se encuentra el hecho de que el titular de los datos no

se hubiera opuesto al mismo por escrito (artículo 18 3º), lo cual difiere de las regulaciones de otros Estados Miembros sobre este asunto.

El artículo 25 recoge la posibilidad de adoptar Códigos de Conducta por distintas entidades, para lo cual necesitarán la aprobación de la Data Protection Commission (Autoridad de Control holandesa).

El deber de información se recoge en los artículos 33 y 34 de esta Norma. Asimismo, regula los derechos de los titulares de los datos, las transferencias internacionales y el régimen de infracciones y sanciones, entre otras obligaciones ya impuestas en la Directiva 95/46/CE.

4.3.11. Irlanda

La primera Ley de protección de datos irlandesa fue de fecha 13 de julio de 1988. Actualmente, está siendo debatido ante el Parlamento un proyecto de ley.

4.3.11.1. Consideraciones a destacar

La Data Protection Act de 1988 es una norma bastante antigua en el tiempo.

En su artículo 1 se define como "dato personal", toda información relativa a una persona viva que pueda ser identificada bien a través de los datos, o por medio de los datos asociados con otra información que esté en posesión del responsable del fichero.

A través de los artículo 4 a 6 se regulan las condiciones para ejercitar el derecho de acceso y rectificación por parte de los titulares de los datos.

Su Autoridad de Control (Comisión) es creada a partir de los artículos 9 y 10.

Otros aspectos regulados son la transferencia internacional de datos; condiciones específicas para la notificación de ficheros o el régimen de infracciones y sanciones.

4.3.12. Italia

La ley de protección de datos italiana es la **Ley 675/96 de 31 de diciembre (Tutella delle persone e di altri soggetti rispetto al tratamento dei dati personali)**. Asimismo, se han aprobado un conjunto de normas en base a la misma, en particular, reales decretos tales como el nº 123 de mayo de 1997; nº 255 de julio de 1997; nº 135 de mayo de 1998 o el más reciente, el nº 282 de julio de 1999.

4.3.12.1. Consideraciones a destacar

Conforme se establece en su artículo 1, esta Norma pretende asegurar que el tratamiento de datos personales se realice respetando los derechos fundamentales y las libertades y dignidad de las personas físicas, con especial atención a su derecho a la privacidad.

Asimismo, como novedad, garantiza los derechos de las personas jurídicas, en esta materia.

Siguiendo los criterios de la Directiva 95/46/CE, algunos de los principios tratados son: calidad de los datos; deber de información; obtención del consentimiento y excepciones; seguridad de los datos, principio que será desarrollado a través de real decreto; transmisiones de datos a terceros; tratamiento de datos sensibles o transferencias internacionales, entre otros.

Específicamente, esta norma recoge qué debe hacerse por el responsable del fichero, una vez que finalice el tratamiento de los datos: destruirlos, transmitirlos a otro responsable o mantenerlos disociados.

4.3.13. Luxemburgo

La primera regulación existente en esta materia en Luxemburgo fue la Ley de 31 de marzo de 1979 (Act Regulating the Use of National Data in Data Processing), la cual ha sufrido varias modificaciones posteriores y el Reglamento del Gran Ducado de 2 de agosto de 1979, sobre la Comisión Consultiva prevista en el artículo 30 de la ley de 31 de marzo.

Actualmente, la **ley vigente** es del año **2002.**

4.3.13.1. Consideraciones a destacar

La Norma protege los derechos fundamentales y las libertades de personas físicas, en particular sus vidas privadas, en cuanto al tratamiento de datos personales, y asegura el respeto de los intereses legalmente protegidos de las mismas (artículo 1).

Conforme a la definición de Procesamiento de datos personales del artículo 2, la ley se aplica a los tratamientos automatizados y no automatizados de datos.

Ya con estas referencias se puede observar una clara tendencia en la consecución de una fiel trasposición del régimen comunitario establecido por la Directiva 95/46/CE.

4.3.14. Portugal

La primera ley de protección de datos portuguesa es de fecha de 9 de abril de 1991 (Ley 10/91). Actualmente, se encuentra en vigor la **Ley 67/98 de 26 de octubre (Lei da Proteccao de Dados Pessoais)**.

4.3.14.1. Consideraciones a destacar

El principio general perseguido por esta Norma se recoge en su artículo 2: el tratamiento de datos personales debe realizarse de forma transparente y con estricto respeto a la vida privada, los derechos, libertades y garantías fundamentales.

Esta Norma no introduce novedades respecto de los principios y obligaciones impuestas por la Directiva 95/46/CE, de manera que alguno de éstos son los siguientes: calidad de los

datos; necesidad de amparar el tratamiento en el consentimiento inequívoco del titular o en alguna de las excepciones recogidas en la Norma; tratamiento especial para los datos sensibles; regulación de las cesiones de datos; derechos de los titulares; deber de información; seguridad; tratamiento de datos por entidades subcontratadas; transferencias internacionales; códigos de conducta; etc.

La autoridad de control en Portugal recibe el nombre de Comissao Nacional de Proteccao de Dados, también llamada CNPD.

4.3.15. Suecia

La primera ley sueca de protección de datos fue la Ley 1973/289 que, posteriormente, se ha visto modificada en 1989.

Actualmente, la ley vigente es el **Personal Data Act (1998/204)**.

4.3.15.1. Consideraciones a destacar

El propósito de esta Norma es proteger a las personas contra la violación de su integridad a través del tratamiento de sus datos personales.

Al igual que el resto de normativas nacionales analizadas, esta protección se asegura a través de una serie de principios y obligaciones que deberán ser adoptados.

A lo largo de la misma, se establecen unos requisitos esenciales para todo tratamiento de datos: legitimidad del tratamiento; determinación clara de las finalidades del tratamiento; solicitud de datos adecuados, pertinentes y puestos al día; obligación general de obtener el consentimiento del titular (salvo excepciones); especiales medidas para el tratamiento de datos sensibles; deber de información; regularización de tratamientos efectuados por terceros, etc.

Como ha podido comprobarse, las principales normas aprobadas por los Estados Miembros sobre esta materia, recogen fielmente las obligaciones, derechos y principios referidos en la Directiva 95/46/CE, de manera que no es frecuente encontrar artículos "novedosos" aplicables de forma específica a IPv6. En este sentido, sería necesario conocer la legislación recogida en estos Estados, de carácter sectorial, como por ejemplo, la legislación de telecomunicaciones, comunicaciones electrónicas, etc.

5. Problemas Prácticos

Una vez que ha sido analizada la legislación vigente en esta materia, a continuación, se expondrán algunos de los problemas prácticos con implicaciones en protección de datos más relevantes, tras la implantación de IPv6.

3 Protección de datos personales

5.1. Nuevos tratamientos de datos como consecuencia del uso de IPv6

El dato de dirección IP podría considerarse como un dato de carácter personal habida cuenta que existe la posibilidad de relacionar dicha dirección IP (a partir del Identificador Único que forma parte de la misma) con el terminal al que identifica y, en consecuencia, podría existir la posibilidad de relacionarla con el usuario titular de dicha IP.

Este hecho, conlleva dos consecuencias y dos ámbitos que, necesariamente, deberán regularse en materia de protección de datos personales:

- Las consecuencias derivadas de la obtención y tratamiento de la dirección IP basada en un Identificador Único, como dato en sí de carácter personal.
- Los nuevos tratamientos de datos que se generarán como consecuencia de la potencialidad de asociar cierta información distinta de la propia dirección IP, que hasta ahora podría ser anónima, con una determinada persona. Por ejemplo, con las direcciones IP asignadas de forma dinámica por un Internet Access Provider y utilizadas a través del actual Protocolo, versión 4, un usuario cada vez que accedía a la Red lo hacía a través de una IP diferente. En una sesión podría acceder a una página web concreta donde se le solicitaran una serie de datos a los efectos de conocer qué tipo de usuarios acceden a dicha página, por ejemplo, su edad y sexo.

  En este caso, si el usuario no aportaba su nombre y apellidos y en el caso de que el portal no tuviera mecanismos de rastreo, cookies, etc, en principio, dichos datos serían anónimos. Como mucho podrían quedar asociados a una dirección IP dinámica, la cual cambiaría para ese usuario en una próxima conexión.

  Por otro lado, es importante indicar que muchos proveedores de acceso proporcionan direcciones estáticas a sus usuarios, y en general, debido a la necesidad de intercepción legal y registro de las transacciones, no hay una situación real de conexión anónima.

Pues bien, con IPv6 dichos datos podrían ser asociados a una determinada IP con Identificador Único que identificaría automáticamente a un terminal y, potencialmente, a un usuario concreto.

Por este motivo, la implantación de IPv6 conlleva que en ambos casos exista, salvo excepciones, un tratamiento de datos nuevo y, por tanto, unas nuevas obligaciones a cumplir por parte de los agentes tratantes involucrados.

Es clave recordar la importancia a este respecto del RFC3041, que como anteriormente se ha indicado, cuando se usa, proporciona un nivel de privacidad superior, no disponible con IPv4.

5.2. Obtención del dato de dirección IP por los agentes tratantes

Uno de los ejemplos en los que el dato de dirección IP es considerado un dato personal, es el tratamiento que del mismo realizan los proveedores de acceso a Internet o los operadores de telecomunicaciones, entre otros agentes tratantes.

A estos efectos, estos agentes tratantes celebran un contrato con los usuarios de sus servicios. En líneas generales, como consecuencia de este contrato, estos agentes tendrán en su poder las direcciones IP de sus usuarios, junto con otro tipo de datos que les son solicitados en la contratación, tales como su nombre, dirección o número de cuenta bancaria.

Asimismo, estos agentes tratantes podrán registrar la fecha de acceso a la Red, la hora y la duración de la conexión efectuada por el usuario.

Por este motivo, es importante afirmar que, en este supuesto, el momento de la contratación se convierte en el canal para que el proveedor asocie la dirección IP a su titular, lo cual conlleva una serie de obligaciones para estos agentes tratantes en materia de protección de datos personales, tales como su consideración como responsables del fichero originado como consecuencia del tratamiento y almacenamiento de estos datos, la obligación de notificar dicho fichero ante la autoridad nacional en protección de datos que corresponda, así como el cumplimiento del resto de obligaciones que han sido expuestas con anterioridad.

Otro de los principales agentes tratantes existentes en Internet, los cuales suelen llevar a cabo un tratamiento del dato de dirección IP asociado al titular de la misma, son los ISP´s (Internet Service Provider), los cuales, como su propio nombre indica, ponen a disposición de los usuarios de Internet, una serie de servicios, de naturaleza diversa.

5.3. Otros medios que permiten considerar la dirección IP como dato personal

5.3.1. Utilización de guías públicas

Hay supuestos en los que, potencialmente, un agente tratante podría cumplir con la prestación de un servicio solicitado por un usuario, sin necesidad de tener que conocer la identidad del mismo que se encuentra detrás de una determinada dirección IP.

En estos casos, aunque el agente tratante, prestador de dicho servicio, mantenga el dato de dirección de IP solicitante del servicio, si este agente no tuviera la posibilidad de cruzar dicho dato con ninguna otra fuente de información relativa al usuario titular, no estaría tratando datos de carácter personal y, por lo tanto, no estaría vinculado por esta normativa, puesto que el mero dato de dirección IP no identificaría a una persona física concreta.

Si bien estas argumentaciones son bastante válidas desde una perspectiva teórica, imaginemos que, al igual que existen actualmente para la telefonía fija, se crearan para IPv6

guías públicas o listados del estilo de las bases de datos Whois (Whois Database), accesibles a todo el mundo, en los cuales se recogiera el nombre y apellidos del usuario junto con la parte del Identificador Único que compondría su dirección IP y a los cuales pudieran tener acceso cualquier agente tratante, por ejemplo, titulares de páginas web o de establecimientos comerciales existentes en Internet.

El mero hecho de que existiera la potencialidad razonable de que los mencionados terceros pudieran cotejar las direcciones IP a las que tuvieran acceso como consecuencia de la prestación de sus servicios, con un listado y conocer quiénes son sus titulares, automáticamente, convertiría estos identificadores únicos de las direcciones IP en datos de carácter personal.

A estos efectos, conviene aclarar que se habla de la posible creación de listados públicos que relacionaran al usuario con la parte del Identificador Único de las direcciones IP puesto que en los casos de terminales con movilidad, su dirección IP entera no sería siempre la misma, ya que parte de ésta se vería modificada en base al lugar donde dicho dispositivo se estaría conectando a la Red. Por el contrario, para aquellos terminales sin movilidad, que acceden a la Red siempre desde un mismo punto, su dirección IP siempre sería la misma.

A continuación, se recogerán una serie de consideraciones relativas a la creación de guías públicas, teniendo en cuenta, entre otras, las consideraciones que se establecen en la Directiva 2002/58. En este sentido, resulta importante matizar que las disposiciones de esta Directiva en relación con las guías de abonados se encuentran directamente enfocadas a los directorios generados para telefonía, es decir, aquellos a través de los cuales es posible asociar una determinada persona a su número telefónico.

En este sentido, salvando las diferencias que este tipo de guías telefónicas pudieran tener respecto de aquellas que pudieran crearse para direcciones IP basadas en Identificador Único, las cuales se pondrán de manifiesto en el presente apartado, a continuación se realizará un breve análisis acerca de la regulación ofrecida por la citada Directiva, respecto de este tipo de guías.

5.3.1.1. Naturaleza de las guías públicas

Una de las primeras diferencias que podría surgir respecto del tipo de guías reguladas a través de la citada Directiva se deriva de la propia naturaleza de las guías o repertorios de direcciones IP que podrían llegar a generarse.

En concreto, el propio carácter extraterritorial de Internet, impregnaría de esta naturaleza extraterritorial a estos repertorios, de manera que se plantea la duda acerca de si estas guías tendrían carácter mundial, comunitario o, incluso, nacional. En este sentido, resultaría importante determinar que el propio sistema de asignación de direcciones IP implantado en la actualidad y que, en principio, parece que no sufrirá cambios sustanciales con el funcionamiento de IPv6, potenciaría la creación de repertorios de direcciones IP de naturaleza mundial.

Por este motivo, las guías de IP que podrían llegar a crearse, podrían ser de naturaleza similar a un cierto tipo de guías existentes en la actualidad, las cuales permiten realizar consultas a través de Internet y conocer, por ejemplo, a través de un nombre de dominio, la entidad o persona que tiene registrado dicho nombre de dominio, el servidor DNS e, incluso, la dirección IP de dicho dominio.

En otras ocasiones, estas guías permiten una asociación inversa, es decir, a través de una dirección IP, facultan a la persona que realiza la búsqueda, conocer qué persona o entidad registró un dominio identificado con una IP determinada.

Por último, junto con la problemática derivada de la naturaleza de estas guías, otro de los temas que deberían tenerse en cuenta, hace referencia a si la elaboración de las mismas se efectuaría en régimen de libre competencia o, por el contrario, se decidiría la creación de un único organismo que se encargaría de la gestión, actualización y tratamiento de las mismas, conforme se exige en la normativa de protección de datos personales.

5.3.1.2. Sistemas de inclusión de los datos en las guías públicas

En principio, la Directiva 2002/58/CE es la normativa con implicaciones en materia de protección de datos que recoge una regulación de guías de naturaleza pública, que si bien no pretende regular las guías de IP que podrían generarse, podría tenerse en consideración, a la hora de elaborar la regulación del uso de este nuevo tipo de repertorios.

Tras el análisis del método de inclusión de los datos en estas guías que recoge la Directiva, parece deducirse que ésta únicamente faculta al titular de los datos para decidir si desea o no, estar incluido en las mismas. Por ello, los sistemas a adoptar para proceder a la inclusión de los datos de un usuario en una guía pública pueden ser de dos tipos:

- Inclusión automática de los datos en la guía, dando cumplimiento al deber de información y consentimiento, de manera que si el usuario no desea figurar en la misma, solicite su baja o,
- Solicitud de inclusión en la misma, de forma expresa, por parte del usuario.

5.3.1.3. Algunos supuestos a regularizar

La creación de este tipo de guías supondría la generación de una serie de dinámicas a regularizar desde la perspectiva de esta normativa. Estas dinámicas, asimismo, se encontrarían influidas por el sistema de asignación de las direcciones IP y, por lo tanto, por las entidades habilitadas para crear listados con los usuarios y sus respectivas direcciones IP (identificadores únicos).

Asimismo, otros de los aspectos importantes desde la perspectiva de protección de datos, sería la forma de alimentar y actualizar estas guías que, en ocasiones, estaría basada en la transmisión de los datos a incluir en las mismas, que los agentes tratantes con facultad para asignar direcciones IP a los usuarios deberían aportar a la entidad o entidades encargadas de su elaboración.

Asimismo, debería regularizarse la posición de esta entidad o entidades y la titularidad de los ficheros generados a partir de la creación de estas guías.

En concreto, ¿quién sería el responsable de los datos contenidos en estas guías: la entidad o entidades que las generen o los agentes tratantes que obtengan tales datos y se los faciliten?. Esta será una de las cuestiones a debatir en el supuesto en el que se adopten estas guías. Cuestión que no es baladí, habida cuenta que dependiendo de qué entidad o entidades se consideren responsables de tales ficheros, se conocerá cuáles de ellas deberán dar cumplimiento a los deberes de información, obtención del consentimiento para la inclusión de los datos en las guías, etc.

Asimismo, en el caso de que no se crearan entidades gestoras de estas guías sino que éstas fueran elaboradas por los propios agentes tratantes con facultad para asignar direcciones IP, éstos serían los que, en todo caso, deberían informar a los titulares de la inclusión de sus datos en la mencionada guía, del tratamiento que sobre los mismos se pretende llevar a cabo así como del resto de parámetros del deber de información, a la vez que será necesario que, en todo caso, obtengan su consentimiento previo.

Por otro lado, también existirían obligaciones de protección de datos para el resto de agentes que trataran dicha información. Es decir, para aquellos que si bien no participarían en la elaboración y/o actualización de la información contenida en las guías, procedieran a utilizarlas para asociar direcciones IP basadas en un Identificador Único con un determinado usuario.

5.3.1.4. Utilización de Guías de búsqueda inversa

La revolución que ha supuesto la informática y la tecnología y con ellas la digitalización de la información ha permitido que surjan nuevas posibilidades de acceso a la información contenida en guías públicas que facilitan la idea de asociar datos personales.

En este sentido, existen numerosos tipo de guías que permiten realizar búsquedas de información de forma inversa. En este sentido, se han elaborado guías inversas o multicriterio que permiten que a través del número telefónico, se obtenga información personal de un determinado sujeto (nombre y apellidos, dirección, etc). Otro ejemplo, son guías generalmente consultadas a través de Internet que permiten obtener cierta información acerca de la entidad o persona que ha registrado un nombre de dominio, a partir de la aportación de este nombre de dominio.

Por la proximidad que revisten este tipo de guías citadas con las que pudieran crearse sobre direcciones IP (a través de la IP se podrían obtener datos de la persona titular de la misma), es conveniente tener en cuenta las consideraciones siguientes.

Estas prácticas de búsqueda inversa han originado una importante inquietud, al menos, respecto de la utilización de guías inversas de carácter telefónico, por un posible atentado al derecho a la intimidad y a la protección de datos de los afectados, lo que en la práctica ha producido que algunas legislaciones nacionales, en materia de telecomunicaciones principalmente, hayan procedido a su prohibición o a la determinación de una serie de requisitos para su creación, en base a las recomendaciones efectuadas por el Dictamen 5/2000 sobre el uso de guías telefónicas públicas para servicios de búsqueda inversa o multicriterio, adoptado el 13 de julio de 2000 por el Grupo de trabajo sobre la protección de las personas físicas en lo que respecta al tratamiento de datos personales.

Este Dictamen reconoce que, en muchos casos, este tipo de guías pueden atentar contra la intimidad de los usuarios, porque se entiende que utilizar las guías públicas que pudieran crearse para averiguar los datos personales del titular del número telefónico, constituye un uso totalmente distinto de aquel que fue pretendido por el titular de los datos al consentir entrar a formar parte de una guía pública.

No obstante, matiza que en otras ocasiones pueden llegar a ser útiles y por tanto, no deberían prohibirse como tales, sino adoptar las medidas previstas en la Directiva 95/46/CE para su regularización: deber de información y consentimiento, principalmente.

Por todo ello, es importante que tomando en consideración estos argumentos y salvando las distancias ya apuntadas, existentes entre las guías telefónicas inversas y las que podrían crearse en relación con direcciones IP, es posible concluir que si bien, la regla general es que se opte por su no generación y uso, en el caso en el que se considere realmente útil su elaboración, en todo caso, deberá llevarse a cabo respetando los principios y obligaciones de la normativa de protección de datos, en concreto, el deber de información y la obtención del consentimiento de los titulares de los datos para su inclusión en la guía y el posterior tratamiento de sus datos conforme a unas finalidades claramente determinadas.

5.3.2. Contrataciones de servicios

Si bien la creación de guías públicas con el listado de direcciones IP podría ser uno de los medios adoptables para relacionar una dirección con su titular, existen otros medios que convierten este tipo de dato en dato personal.

Para ciertos agentes tratantes, a la hora de contratar por el usuario un determinado servicio, es requisito fundamental la obtención de la dirección IP con Identificador Único para poderle prestar el servicio correctamente, por ejemplo, pensemos en el proveedor de acceso a Internet.

En este caso, este agente tratante tendrá la relación IP-Usuario contratante a través del contrato.

Otro ejemplo, se deriva de la posibilidad de que los electrodomésticos de nueva generación incorporen direcciones IP basadas en Identificadores Únicos. Esto abre nuevas posibilidades, por ejemplo, a las cadenas de supermercados a que comiencen a prestar servicios que supongan el envío automático de los productos que el citado electrodoméstico le hubiera solicitado, una vez que hubiera detectado su falta.

En estos casos, puede ocurrir que el proveedor de estos servicios necesite asociar la dirección IP con, al menos, la dirección a la que debe remitir el pedido y, por lo tanto, con el titular de la misma que deberá abonar dicho pedido.

En estos casos, será frecuente que el medio de obtención de estos datos sea a través de la celebración del oportuno contrato con el usuario.

Por este motivo, para los prestadores de servicios de esta naturaleza podría entenderse que el dato de dirección IP sería un dato de carácter personal ya que la asociación de dicha dirección IP con su usuario titular, sería llevada a cabo por el prestador del servicio a través del contrato celebrado entre ambos.

Por lo tanto, este contrato, se convierte en el medio idóneo a utilizar por el prestador de servicios (agente tratante) para dar cumplimiento a sus deberes de información y de obtención del consentimiento para el tratamiento y posible cesión de los datos del usuario, contratante de sus servicios.

5.4. Posibilidad de "portabilidad" en las direcciones IP con Identificador Único

Otro de los problemas jurídicos que podrían plantearse está basado en quien o qué entidad será la encargada de otorgar este tipo de direcciones IP y, asimismo, en el caso de que fueran otorgadas por el proveedor de acceso o por la operadora de telecomunicaciones, si dichas direcciones serán las mismas para cada usuario o podrán variar si dicho usuario cambiara de proveedor de acceso o de operadora.

El hecho de que estas direcciones no tuvieran el carácter de "propias y permanentes" para cada uno de los usuarios, conllevaría la necesidad de llevar a cabo ciertas actividades relevantes desde el punto de vista de la protección de datos, que deberían regularizarse.

Por ejemplo, la obligaciones de actualizar las guías públicas que pudieran generarse sobre esta materia y la necesidad de que los proveedores de acceso, operadoras de telecomunicaciones y cualquier otro agente tratante comuniquen las modificaciones efectuadas sobre la titularidad de estas IP´s.

En estos supuestos, deberían crearse disposiciones que regularan o, al menos, aportaran criterios para proceder al tratamiento de los datos conforme a la normativa vigente.

5.5. Posibilidad de rastrear la navegación de los usuarios

Uno de los principales problemas que han sido detectados con respecto a la implantación de las direcciones IP basadas en un Identificador Único, es el hecho de que es posible rastrear la navegación y actividades realizadas por el usuario conectado a la Red (lo cual ya era posible en la versión del Protocolo IP anterior a través de cookies, mecanismos espía, etc), pero la novedad se basa en el hecho de que los resultados de dicho rastreo pueden asociarse a un terminal y, potencialmente, a su titular o persona que los ha llevado a cabo.

Si bien, una de las principales premisas de la normativa analizada es que los tratamientos de datos personales se efectúen con una serie de garantías para el titular de los mismos, esta posibilidad permitida por IPv6 abre las puertas a nuevos tipos de tratamientos que, hasta ahora, no tenían la necesidad de ser regularizados.

Por ejemplo, un rastreador con capacidad de asociar la información a su titular, podría llegar a conocer, por ejemplo, los lugares o páginas web visitadas por éste, las horas de conexión y de desconexión, los objetos o servicios adquiridos, las compras realizadas, por ejemplo, a través de las solicitudes efectuadas al supermercado por su nevera, e incluso, la localización del terminal desde el cual se estarían efectuando las comunicaciones correspondientes.

Sin embargo, analizando este supuesto desde otra perspectiva, tal vez menos alarmista, es posible darnos cuenta de que en el momento en el que un usuario obtenga una determinada dirección IP basada en un Identificador Único, comenzará a ser consciente de la posibilidad de que se efectúen este tipo de tratamientos sobre su información personal y, además, debería ser informado de ello por los distintos agentes tratantes. En consecuencia, deberá exigir a su proveedor la adopción de medidas técnicas que faciliten la preservación de su identidad (i.e. RFC3041).

En este sentido, la Posición Común respecto a la elaboración de perfiles en línea en Internet, adoptado en el 27 Encuentro del Grupo de Trabajo de Berlín, en Creta el 4/5 de Mayo de 2000, establece para los proveedores de servicios de Internet, la obligación de notificar a los usuarios, en todo caso, el tipo, propósito, lugar, duración del almacenamiento, recogida, tratamiento y uso de los datos con la finalidad de obtener perfiles del usuario. Incluso, esta obligación va más allá, al exigir a los proveedores que este deber de información deberá cumplirse aunque los datos recogidos se asociaran a un pseudónimo.

Protección de datos personales

5.6. ¿Qué medios pueden existir para dar cumplimiento al deber de información por los agentes tratantes?

Realmente, no se plantean, en principio, problemas distintos acerca del cumplimiento del deber de información por parte de los agentes tratantes que no existieran con versiones anteriores de este Protocolo.

En los casos en los que se efectúe una contratación con el usuario y se pretenda conservar su dirección de IP para determinadas finalidades, deberá incluirse una cláusula informativa en dicho contrato.

Si por el contrario, dicha obtención y tratamiento se efectúa a través de la navegación, por medio de cualquier tipo de dispositivo conectado a la Red, deberá introducirse la cláusula informativa correspondiente en cada una de las páginas web accedidas, cuyo titular pretenda tratar este dato personal.

En este sentido, es importante resaltar que si un determinado agente tratante hubiera informado al titular de la dirección IP de cada uno de los aspectos determinados por la Directiva, incluidas las finalidades del tratamiento de sus datos previstas, en el caso de que con posterioridad decidiera tratarlos para finalidades distintas o nuevas, deberá volver a informar de ello a los titulares de los datos, así como obtener el debido consentimiento (tácito en unas ocasiones y expreso en otras) de éstos.

En definitiva, respecto del cumplimiento de esta obligación, así como de otras contenidas en nuestra legislación vigente, no se encontrarían especialidades respecto del modo o del medio para informar. Tal vez, el principal cambio se debe a que serán más el número de agentes tratantes que deban informar, al pasar a considerarse este dato, como un dato de carácter personal.

5.7. Movilidad en IPv6

Cuando se habla de "movilidad en IPv6", debemos entender todos aquellos dispositivos que tienen la posibilidad de conectarse a la Red a través de distintos puntos, de manera que es como si "se movieran a lo largo de la Red" (por ejemplo, ordenadores portátiles, terminales de telefonía móvil, PDA´s, etc). Es decir, se trata de cualquier dispositivo que pueda conectarse en un punto u otro punto de la Red sin perder su dirección IP.

Pensemos en el ordenador portátil de un ejecutivo, éste puede conectarse a la Red desde su oficina, desde su casa, desde el hotel donde se aloja, etc.

Para este tipo de dispositivos, es frecuente preguntarse si sus direcciones IP, basadas en IPv6, contienen la parte de Identificador Único y, por lo tanto, si a partir de las mismas,

existe la posibilidad de identificar el dispositivo y la potencialidad de conocer a su titular.

En este caso, sí es posible que este tipo de direcciones se den para dispositivos móviles, cómo es posible conocerlas si éstos se conectan a la Red desde distintos lugares físicos, teniendo en cuenta que cuando estos dispositivos se mueven por la Red, generan nuevas direcciones como consecuencia de su nuevo punto de conexión.

Sin embargo, es importante resaltar que aunque parte de su dirección se ve modificada, el Identificador Único contenido en la dirección, se mantiene igual. De este modo, es posible identificar el dispositivo.

Como es lógico, esto plantea problemas más allá de la mera identificación del usuario, como por ejemplo, la posibilidad de conocer, con bastante acierto, su localización geográfica, ya que una dirección IP puede ser un dato de localización, como se determina en el apartado 4.2.4.

Además, puesto que los datos de localización son datos de tráfico, tanto los operadores de telecomunicaciones como los ISPs, tienen la obligación de proceder a su retención para la persecución de actividades contrarias a la ley. En estos casos, si bien la intimidad de los usuarios podría verse afectada, éstos deberán tener en cuenta que este tratamiento está obligado por ley y que su capacidad para limitarlo se encuentra claramente reducida.

En este sentido, la Directiva 2002/58/CE permite que los Estados miembros determinen las medidas para llevar a cabo dicha retención de datos de tráfico. Así, su artículo 15 establece que *"los Estados miembros podrán adoptar medidas legales para limitar el alcance de los derechos y las obligaciones que se establecen en los artículos 5 (Confidencialidad de las comunicaciones) y 6 (Datos de tráfico), en los apartados 1 a 5 del artículo 8 (Presentación y restricción de la identificación de la línea de origen y de la línea conectada) y en el artículo 9 (Datos de localización distintos de los datos de tráfico) de la presente Directiva, cuando tal limitación constituya una medida necesaria, proporcionada y apropiada en una sociedad democrática para (...) la prevención, investigación, descubrimiento y persecución de delitos (...). Para ello, los Estados miembros podrán adoptar, entre otras, medidas legislativas en virtud de las cuales los datos se conserven durante un plazo limitado justificado por los motivos establecidos en el presente apartado".*

El mismo artículo señala que la adopción de tales medidas se adecuará a lo establecido en la Directiva 95/46/CE y que, además, el Grupo del Artículo 29 velará porque dichas medidas sean conformes a la protección de los derechos y libertades fundamentales y de los intereses legítimos en el sector de las comunicaciones electrónicas.

En consecuencia, la utilización de dispositivos con movilidad que hagan uso del protocolo IPv6 requiere tener en cuenta ciertos aspectos jurídicos, en gran medida similares a los que se han de tener en cuenta actualmente cuando el protocolo utilizado es IPv4.

Protección de datos personales

Así, por ejemplo, supongamos que estamos utilizando un dispositivo móvil con IPv6 que dispone, en un solo equipo, de características típicas de un ordenador personal, un teléfono móvil, una PDA y un GPS. El dispositivo es adquirido a un proveedor de telecomunicaciones que actúa también como ISP y que gestiona una plataforma de servicios propios y servicios prestados por terceras partes.

El proveedor del dispositivo deberá obtener el consentimiento informado del usuario con relación a los tratamientos de datos que vayan a realizarse como consecuencia de la utilización del dispositivo móvil, tanto datos de tráfico como cualesquiera otros que se indique.

De tal manera, el proveedor deberá haber previsto, por ejemplo, en el momento de adquisición del dispositivo y a través de un contrato, la regulación necesaria en cuanto a tratamiento de datos personales, referida, al menos, a qué datos se van a tratar, con qué finalidad, durante cuánto tiempo, qué otras partes (además del proveedor) van a acceder a los mismos, qué fines diferentes a los de gestión de datos de tráfico podrán llevarse a cabo, qué obligaciones legales de retención de datos existen, cómo podrá el usuario pedir el cese temporal de la recogida de datos o cómo podrá ejercitar sus derechos con relación a dichos datos. El consentimiento se extenderá, únicamente, sobre los tipos de datos y tratamientos de los que expresamente se haya informado al usuario.

Otra situación, relativa al tratamiento de datos de localización distinta a los datos de tráfico, sería, por ejemplo, aquella en que se combinan las características de localización del dispositivo, a partir de la red a que se encuentre conectado, y GPS, para crear la ruta de un viaje o un desplazamiento del usuario en su vehículo.

En este caso, la Directiva 2002/58/CE establece que únicamente podrán tratarse los datos de localización del usuario distintos a los de tráfico, de manera personalizada, si se ha obtenido el consentimiento del usuario, en la medida y por el tiempo necesario para la prestación de un servicio de valor añadido (por ejemplo, incorporando información sobre los lugares por donde se está pasando, estado de la circulación de vehículos, rutas alternativas, etc.). Conforme indica la Directiva, el proveedor del servicio deberá informar a los usuarios o abonados, antes de obtener su consentimiento, del tipo de datos de localización distintos de los de tráfico que serán tratados, de la finalidad y duración del tratamiento y de si los datos se transmitirán a un tercero a efectos de la prestación del servicio de valor añadido. Igualmente, el usuario deberá contar con la posibilidad de retirar el consentimiento para el tratamiento de dichos datos y disponer de un método sencillo y gratuito para rechazar temporalmente el tratamiento de tales datos para cada conexión a la red correspondiente o para cada comunicación realizada.

En otro supuesto, igualmente utilizando el dispositivo móvil incorporado al vehículo del usuario, podemos plantear qué pasa si el vehículo es robado. En este caso, en primer lugar,

las autoridades competentes podrían utilizar la posibilidad de acceder a datos de tráfico relativos al dispositivo robado para lograr su localización física. Incluso, con el consentimiento informado del usuario, se podría acceder remotamente al dispositivo para, por ejemplo, a través de una cámara web incorporada al dispositivo, saber qué está pasando en el vehículo y proceder a su detención.

En este supuesto, el proveedor de telecomunicaciones debería adoptar el compromiso de no atribuir al usuario, como datos personales, los generados desde el robo del dispositivo móvil hasta su recuperación y poner a disposición de las autoridades todos los datos generados por la utilización del dispositivo por quien lo robó (servicios utilizados, coste, duración, imágenes grabadas, borrado de datos grabados en el dispositivo, etc.).

Por último, cabe plantear, de manera aproximativa, qué implicaciones tiene el hecho conectar el dispositivo móvil a una red distinta a la habitual, con relación al tratamiento de datos personales. Por ejemplo, cuando se conecta a la red inalámbrica gratuita de un aeropuerto para gestionar un billete de avión. En este caso, el proveedor de la red inalámbrica deberá acordar con el usuario, mediante una cláusula de información y consentimiento, que deberá ser aceptada previamente a la utilización del servicio, todos los términos relativos a tipos de datos a tratar, finalidad, duración del tratamiento, etc., inclusive el hecho de que el dato de la IP basada en IPv6 y los datos que se generen asociados al mismo sólo se tratarán a efectos del acceso a la red inalámbrica.

Una vez esto, por ejemplo, el usuario comienza a gestionar su billete de avión, y debe realizar una videoconferencia con la compañía aérea para solucionar una incidencia. En este caso, se estaría utilizando la IP del usuario, de manera simultánea para una comunicación con telefonía móvil y un acceso a red inalámbrica. Recordemos que los tratamientos de datos han sido acordados, de manera separada y para cada servicio, con el operador de telecomunicaciones y con el proveedor de la red inalámbrica. Lo más relevante en este caso es el compromiso, contractual y técnico, de ambos operadores de que sólo asociarán a la concreta IP los datos relativos a su propio servicio, y no realizarán un cruce de datos por el hecho de que el usuario esté utilizando dos servicios diferentes de manera simultánea y haciendo uso de la misma IP o de dos IPs con un mismo Identificador Único.

En definitiva, podemos ver como, aunque la definición de los tratamientos personales variará en función de los servicios que establezcan, la utilización de dispositivos móviles con IPv6 genera una serie de tratamientos de dichos datos, en todo caso, que deberá adecuarse a los principios que se desarrollan a lo largo de esta Parte y cuyas fuentes principales son, actualmente, la Directiva 95/46/CE y la Directiva 2002/58/CE.

Protección de datos personales

5.8. IPv6 y Domótica

Uno de los sectores donde más aplicación están teniendo los avances logrados durante estos últimos años por la Domótica es en el hogar y, en concreto, en los electrodomésticos. En este sentido, ha llegado a definirse la Domótica como "el uso simultáneo de la electricidad, la electrónica y la informática, aplicadas a la gestión técnica de las viviendas".

En concreto, algunos de los objetivos perseguidos por estos avances son:

- Ahorro energético: control de temperatura, iluminación, consumos, etc.
- Seguridad: custodia y vigilancia frente a la intrusión, la inundación, el fuego, los escapes de gas, pero también la seguridad personal, etc.
- Comunicaciones: telecontrol y telemetría, acceso a Internet, comunicación interna y compartición de recursos informáticos dentro del hogar.
- Confort: programaciones horarias calefacción, escenarios luminosos, riego automático, etc.

Para ello, la Domótica usa multitud de dispositivos que pueden ser distribuidos por toda la vivienda en función de las necesidades de los propietarios. Básicamente, estos dispositivos se pueden dividir en sensores y actuadores con inteligencia suficiente como para implementar "una red de área local" de control distribuido.

Respecto al presente estudio, interesa conocer qué implicaciones pueden existir en el uso del protocolo IPv6 en electrodomésticos de esta categoría.

Por ejemplo, en el caso de que los distintos aparatos o dispositivos de Domótica existentes en una casa tuvieran cada uno de ellos una IP para acceder a la Red, con Identificador Único, aquellos agentes tratantes que tuvieran la posibilidad de acceder a los resultados de dicha navegación o acceso, podrían obtener información tan valiosa como los perfiles de consumo de los titulares de la casa, sus horarios, sus gustos, etc.

Asimismo, esta posibilidad aumentaría si fuera posible que todos los dispositivos o nodos existentes en una casa tuvieran el mismo prefijo en su dirección IP, siendo un identificador constante.

Sin embargo, desde el punto de vista de la protección de datos, es importante resaltar que:

- Las actividades de generación de perfiles, de forma inconsentida, es un problema que viene existiendo con las anteriores versiones del Protocolo y que, por lo tanto, no es un problema iniciado por el uso de IPv6.
- No es una actividad sencilla para un único agente tratante, acceder a estas IP´s e incluso agrupar todas aquellas que existan en una casa, para obtener perfiles.

- La obtención de perfiles es lícita si se efectúa dando cumplimiento a las disposiciones contenidas en la Directiva y en las legislaciones de cada Estado Miembro, adoptadas sobre protección de datos.
- No en todos los casos, la dirección IP que para un agente tratante tiene la consideración de dato personal, tiene que serlo para otro agente o prestador de servicios distinto.

En el supuesto de que la dirección IP pueda tener la consideración de dato personal y pensando en aquel caso que, existiendo o no un prefijo único para todos los elementos de la Domótica de un hogar, es posible conocer el usuario de una IP (por ejemplo, mediante guías públicas), los requisitos derivados del tratamiento de datos personales pueden ser diferentes en función del uso o servicio proporcionado por el elemento de la Domótica.

Podemos pensar el caso de un de un equipo terminal con una dirección IP propia y que es utilizado para la prestación de un servicio de teleasistencia sanitaria para todos los miembros de la familia, accesible a través de la identificación individualizada de los mismos mediante un dispositivo biométrico.

De manera simplificada, en la prestación del servicio intervendrían tres partes: el proveedor de las telecomunicaciones necesarias, el proveedor del servicio (que provee también el dispositivo) y los usuarios.

En cuanto al proveedor de telecomunicaciones, los datos que podría asociar a la IP basada en IPv6 del dispositivo domótico serían los necesarios para la gestión, facturación y cobro del tráfico generado en su utilización y, en su caso, aquellos otros datos que hubiera acordado con el titular del dispositivo que podrían ser recabados y tratados.

Respecto a este segundo tipo de datos, el proveedor de telecomunicaciones tendrían que haber informado al usuario sobre qué datos son, con qué fin se recaban, durante cuánto tiempo van a ser tratados, qué otras partes van acceder a los mismos y cómo podrá el usuario ejercitar sus derechos sobre los mismos. A continuación, se deberá obtener el consentimiento del usuario sobre cada uno de los extremos citados. Se podría dar cumplimiento a ambas obligaciones a través de la inclusión de las cláusulas oportunas en el contrato que regule el uso de las telecomunicaciones asociadas al uso del dispositivo de teleasistencia.

El proveedor del servicio y del dispositivo tiene también que dar cumplimiento a las obligaciones de información y consentimiento relativas a los datos personales que se deban tratar en el uso del servicio de teleasistencia. Sin embargo, normalmente, este proveedor va a tener unos requisitos adicionales.

Así, puesto que es muy probable que se efectúe un tratamiento de datos de salud de los miembros de la unidad familiar que hagan uso del servicio de teleasistencia (por ejemplo, toma de tensión o temperatura, comunicación de síntomas, comunicación de medicación, etc.)

se requeriría la obtención de un consentimiento explícito. Este consentimiento deberá obtenerse de cada uno de los miembros de la familia (salvo en el caso de hijos que se encuentren bajo la patria potestad de sus padres), mediante el contrato de teleasistencia o mediante acuerdos o cláusulas diferentes.

Como se ha señalado, uno de los temas jurídicos más repetidamente planteados con relación al uso de la Domótica es el relacionado con la creación de perfiles referidos tanto a una unidad familiar como a los miembros individuales de la misma. Por ejemplo, podemos pensar qué consideraciones jurídicas habría que tener en cuenta en la creación de ambientes personalizados en dormitorios (por ejemplo, máquinas de estado que determinen intensidad de luz, temperatura, control de persianas, programación de la televisión, etc.) y su combinación con hábitos de alimentación asociados al mes del año que corresponda. Además, podemos pensar que estos servicios están asistidos por una empresa externa que gestiona la correcta creación de ambientes, el aprovisionamiento automatizado de alimentos y la lectura de etiquetas RFID (Radio-Frecuency Identification) de la ropa de los usuarios y de determinados alimentos.

Recordando lo que se ha venido señalando en cuanto a información y consentimiento, podemos centrarnos ahora en la cuestión de la creación de perfiles. Como se ha señalado, la creación de perfiles es lícita si se efectúa conforme a la Directiva 95/46/CE y, lógicamente, conforme a la normativa de cada Estado Miembro sobre datos personales.

No obstante, el usuario dispondrá siempre de sus derechos de acceso, rectificación, cancelación y oposición, reconocidos por la propia Directiva para, por ejemplo, eliminar los datos de su perfil (datos de la persona asociados a la IP basada en IPv6 y a los elementos de la Domótica de su hogar) obtenidos hasta una determinada fecha, evitar que se modifique la temperatura de un dormitorio a partir de la lectura de las etiquetas RFID de su ropa, limitar el reaprovisionamiento automático de ciertos alimentos (por ejemplo, alimentos especiales, alimentos para dietas por tratamiento médico, alimentos de temporada, etc.), o evitar que la programación de la televisión incluya contenidos no aptos para menores.

Existe otro aspecto importante, relativo al proveedor que está gestionando la creación de ambientes personalizados y el reaprovisionamiento automático de alimentos basado en el mes en curso. Este proveedor, normalmente, va a utilizar los servicios de otras partes para, por ejemplo, generar y entregar un pedido virtual basado en lectura de etiquetas RFID o códigos de barras, fotografía digital de una nevera, etc.

En el caso de que estas terceras partes, para prestar su servicio, tengan acceso a los datos del usuario asociados a su IP, por ejemplo, de su nevera (porque gestionan el reaprovisionamiento de la misma), deberán regular tal circunstancia en el contrato que rija la relación entre el proveedor principal y éste proveedor que ha sido subcontratado por el mismo.

La regulación contractual deberá indicar, al menos, qué datos de IP del usuario basada en IPv6 van a ser tratados para gestionar el servicio, cómo transmitirá el proveedor principal sus órdenes al subcontratado o qué sucederá con los datos (de IP y demás datos personales asociados a la misma) una vez finalice el servicio.

En conclusión, el uso de la Domótica mediante dispositivos basados en IPv6 viene a continuar con los problemas y soluciones jurídicas que suceden con IPv4. No obstante, el desarrollo del nuevo protocolo puede ser un buen momento para plantear y regular los aspectos relativos al tratamiento de datos personales derivado del uso de tales dispositivos basados en IPv6.

5.9. Medidas de seguridad a implantar en el tratamiento de datos de IP

Las Directivas de protección de datos obligan a los distintos responsables de los tratamientos a adoptar las medidas técnicas y organizativas necesarias que, además de garantizar la confidencialidad de la información y su correcto tratamiento, aporten, asimismo, seguridad.

En este sentido, no se determina en ninguna de ellas un conjunto aproximativo de medidas de seguridad a tener en cuenta por los Estados Miembros, lo cual, a efectos prácticos, produce que, en ocasiones, los Estados Miembros dispongan de mecanismos jurídicos de desarrollo de esta obligación pero con un contenido distinto entre unas normativas y otras.

Respecto a la implantación de medidas de seguridad, únicamente resaltar que el nuevo Protocolo IPv6 dispone de una opción de seguridad específica denominada IPSec, a través de la cual se garantiza, entre otros asuntos:

- La autentificación en el origen de los datos y, por lo tanto, la posibilidad de no recibir comunicaciones provenientes de usuarios con una IP determinada
- La integridad de la información transmitida a partir de este Protocolo
- La confidencialidad de la misma

En este sentido, apuntar que las consideraciones acerca de este estándar de seguridad IPSec serán objeto de especial análisis el último bloque de este libro, habida cuenta de las implicaciones que su adopción puede conllevar en la lucha contra la piratería y en la defensa de los derechos de propiedad intelectual, copyrights, etc.

6. Utilización del RFC3041

6.1. Breve explicación de su funcionamiento

Tal y como se determinaba en el Capítulo anterior, en relación con los identificadores únicos de las direcciones IP, IPv6 ha permitido por primera vez que los identificadores de interfaz

puedan formarse de forma automática en los dispositivos, como una de las maneras existentes para crear direcciones. Por lo tanto, los asuntos relacionados con la privacidad se derivan de que éstos se encuentran de forma permanente en las direcciones, permitiendo la trazabilidad de los sujetos titulares de dichos dispositivos.

Existen numerosos tipos de empresas destinadas a realizar estudios de mercado, sirviéndose para ello de variados tipos de técnicas (data-mining) que permiten realizar seguimientos del uso de Internet y, en los casos en los que las direcciones IP no cambien, asociar la navegación y actividades realizadas con los titulares de dichas direcciones. Este hecho es especialmente importante en relación con la proliferación de dispositivos de nueva generación conectados a Internet (por ejemplo, PDAs, teléfonos móviles, etc.) los cuales podría llegar a ser asociados con sus titulares. En este sentido, es importante tener en cuenta que con la proliferación de enlaces "always-on" (DSL, cable modems), aumenta la posibilidad de que los usuarios puedan ser sometidos a actividades de data-mining y al seguimiento de sus direcciones fijas.

Thomas Narten y Track Draves de Microsoft Research publicaron un procedimiento que pretendía tratar este tema y asegurar la privacidad de los usuarios de IPv6 - RFC3041 titulado "Extensiones de privacidad para la autoconfiguración de direcciones sin estado en IPv6" ("Privacy Extensions for Stateless Address Autoconfiguration in IPv6"), el cual fue publicado en enero de 2001 por el IETF. Este procedimiento se basa en la existencia de un algoritmo creado por Narten y Draves, a través del cual se generan identificadores de interfaz aleatorios y direcciones temporales para una sesión de usuario en lo que respecta a comunicaciones salientes. En este sentido, estos identificadores aleatorios sustituyen el identificador único de la dirección, siendo el RFC3041 el medio para estandarizar cómo y cuándo es posible realizar esta actividad.

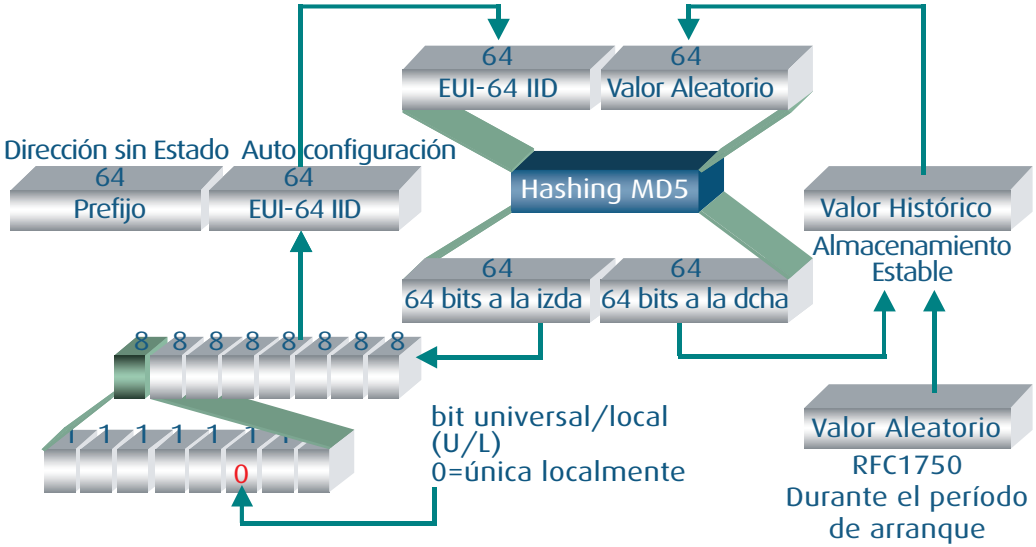
El principal objetivo de este documento era reducir la preocupación acerca de que IPv6 pudiera significar un peligro para la privacidad, mediante la creación de un identificador aleatorio para las comunicaciones salientes. De este modo, se dificulta la posibilidad de relacionar el nodo con su titular.

El resumen inicial de este documento establece lo siguiente:

"Los nodos utilizan la autoconfiguración de direcciones sin estado para generar direcciones sin la necesidad de utilizar un servidor Dynamic Host Configuration Protocol (DHCP). Estas direcciones son creadas a partir de la combinación de prefijos de red con un identificador de interfaz. En los interfaces que contienen Identificadores IEEE, el identificador de interfaz se deriva de éste. Sin embargo, en otro tipo de interfaces, el identificador de interfaz se genera a través de otros mecanismos, por ejemplo, a través de la generación aleatoria. Este documento hace referencia a la autoconfiguración de direcciones sin estado cuyo iden-

tificador de interfaz se deriva de un identificador IEEE. Esta situación implica que los nodos generen direcciones globales a través de identificadores de interfaz que varían, incluso en los casos en los que el interfaz contenga identificadores IEEE. El cambio del identificador de interfaz (y de la dirección global generada a raíz de éste) dificulta claramente que los rastreadores y cualquier otro tipo de entidad o persona dedicada a recabar información, pueda identificar en qué casos direcciones diferentes usadas en transacciones distintas, se corresponden con el mismo nodo".

La autoconfiguración de direcciones sin estado es un mecanismo que genera direcciones basadas en IPv6 de 128 bits. La parte de la izquierda de la dirección está compuesto por 64 bit y se llama "prefijo" y los 64 bits de la parte derecha constituyen el identificador único o EUI-64 IID.



¿Cómo se crea un Identificador de Interfaz siguiendo el RFC3041?

Tal y como se aprecia en el diagrama superior, un número aleatorio reemplazará al EU1-64IID. El mecanismo vinculará un valor aleatorio de 64 bit al EUI-64 IID y un algoritmo hash tendrá lugar. Este es un algoritmo de un solo sentido por lo que no permitirá reconstruir el número original. Por el contrario, este algoritmo generará aleatoriamente un número de 128 bits. Los 64 bits de la parte izquierda de la dirección forman parte de la autoconfiguración de la dirección dinámica (la cual no estará relacionada con el dispositivo ya que el número ha sido generado aleatoriamente, no estando basado en ningún identificador único) para crear una dirección de IPv6 y el identificador de la derecha permanece almacenado de forma fija para evitar duplicaciones. Esta dirección será utilizada para comunicaciones salientes.

Por lo tanto, se utilizarán dos direcciones: una dirección "n" generada en base a la dirección única MAC, utilizada para comunicaciones entrantes (el terminal siempre se encontrará localizable a través de esta dirección permanente), y otra dirección generada a través del RFC3041 de una forma aleatoria, la cual será utilizada para comunicaciones salientes. Por lo tanto, cuando el Terminal (y el usuario que se encuentra detrás del terminal) es responsable de la conexión efectuada, éste no podrá ser identificado a través de la dirección MAC.

En todo caso, parece deducirse que si este RFC se implementara de forma general, estaría facilitando una solución a los problemas en materia de privacidad descritos con anterioridad.

6.2. ¿Cuál es su grado de obligatoriedad?

El RFC3041 se encuentra en la "carrera para convertirse en un estándar", estando englobado en la actualidad en la categoría de "propuesta de estándar" (PS), es decir, se encuentra en uno de los tres niveles definidos hasta obtener la categoría de estándar.

Puesto que actualmente este RFC es una propuesta de estándar, se ha llegado a cuestionar su grado de obligatoriedad y su fuerza vinculante.

Sin embargo, es necesario tener en cuenta que en relación con Internet se han hecho importantes desarrollos que se utilizan en el funcionamiento diario de Internet (PPP, POP3, IPv6, FTP y extensiones TCP, etc.) las cuales se encuentran todavía dentro de la categoría "PS", siendo esto así como consecuencia de que el proceso de aprobación del IETF es bastante lento. Por todo ello, muchos de estos desarrollos pasan a considerarse en la práctica como estándares aunque realmente no tengan esa categoría, como consecuencia de su aceptación generalizada y a obtener "de facto" un status de estándar. En concreto, el RFC3041 ya ha sido implementado en sistemas operativos tan potentes como Microsoft Windows XP/2003 y Linux y su fuerza e importancia habla por sí misma.

6.3. Implicaciones de su adopción desde la perspectiva de protección de datos

Si la adopción de esta medida impidiera a ciertos agentes conocer el Identificador Único de una determinada dirección IP, en principio, podría afirmarse que dicha dirección no sería posible asociarla por el agente tratante a un determinado dispositivo y, por lo tanto, a un concreto usuario y, asimismo, tampoco le facultaría para rastrear sus movimientos a lo largo de la Red.

En consecuencia, el dato de dirección IP, para dicho agente tratante, no tendría la consideración de dato personal y, por lo tanto, éste no quedaría obligado al cumplimiento de las obligaciones impuestas por la normativa de protección de datos personales ya que,

en estas circunstancias, dicha información tendría una consideración de dato anónimo o, al menos, disociado.

Estas afirmaciones serán realmente así en el caso de que dicho agente no tuviera medios alternativos para poder identificar el dispositivo al que corresponde dicha dirección IP.

Por otro lado, a pesar de la utilización de esta medida, necesariamente otros agentes deberán seguir conociendo la dirección IP verdadera que contenga el Identificador Único, por lo que para ellos, seguirían existiendo las obligaciones impuestas en esta normativa.

Si bien esta medida técnica sería aplicable en la mayoría de los supuestos, se ha determinado que el RFC3041 no es aplicable a IP´s con movilidad, por lo que en estos casos, continuarían existiendo implicaciones en esta materia para los agentes tratantes de este tipo de IP´s.

6.4. Implantación por los fabricantes de hardware y software

Siguiendo las recomendaciones efectuadas por el Grupo del Artículo del 29, los fabricantes deberán adoptar las medidas necesarias para la implantación de las medidas técnicas existentes en cada momento, que garanticen la privacidad de los usuarios.

Asimismo, la propia Directiva 2002/58/CE, en su Considerando 46 establece que *"puede ser necesario adoptar medidas que exijan a los fabricantes de determinados equipos utilizados en los servicios de comunicaciones electrónicas que fabriquen sus productos de manera que incorporen salvaguardias para garantizar la protección de los datos personales y la intimidad del usuario y del abonado"*.

En este sentido, sería recomendable que los fabricantes, tanto de software como de hardware, facilitaran a los usuarios la posibilidad de utilizar este tipo de dispositivos o acceder a la Red obviándolos. De esta manera, deberían informar a través de cláusulas informativas estandarizadas de las posibilidades conferidas por estos mecanismos y las consecuencias de su utilización.

En este sentido, al margen de las posibles dificultades de carácter técnico que pudieran existir para su implementación, cabrían varias posibilidades distintas a adoptar por estos fabricantes:

- **Sistema OPT OUT**: según este sistema todos los fabricantes, de forma obligada, deberían introducir en los elementos hardware o software que elaboren, dispositivos de esta naturaleza basados en el RFC3041 o en cualquier otro estándar de esta naturaleza. Si el usuario no deseara utilizar este tipo de herramienta, debería solicitar su "desactivación" al fabricante o proveedor correspondiente.
- **Sistema OPT IN**: por el contrario, esta nueva modalidad supondría que los fabricantes no incluirían de forma generalizada este tipo de herramientas en los elementos hardware

o software que generen pero, en cambio, quedarían obligados a dar la opción a los usuarios de los mismos de adquirirlas, informándoles detenidamente del modo de uso y de las consecuencias de su utilización.

- **Sistema Intermedio**: a través de este sistema, los fabricantes podrán dar la posibilidad a los usuarios adquirientes de sus productos de activar o desactivar la solución técnica, según deseen que su acceso sea anónimo o no.

Esta última opción se presenta, en principio, como la más idónea ya que en determinadas ocasiones será necesario que el usuario acceda a través de una IP reconocible, a los efectos de que el prestador del servicio pueda reconocerle y proveerle aquello que el usuario solicita.

6.5. Otras consideraciones

La adopción del tipo de direcciones IP generadas a partir del Identificador Único han suscitado ciertos comentarios basados en el hecho de que, al margen de las implicaciones respecto de la privacidad de los usuarios, éstas contradicen una de las principales características de Internet: su carácter anónimo.

Por este motivo, el desarrollo de medidas técnicas del estilo de las propuestas por el RFC3041 han tenido, en principio, una buena acogida por ciertos sectores. No obstante, se han planteado ciertas dudas sobre su utilización, por ejemplo, el hecho de que estas medidas podrían llegar a entorpecer investigaciones policiales o judiciales derivadas de la comisión de actividades infractoras o delictivas.

En este sentido, sería conveniente analizar qué agentes tratantes dentro de Internet, por ejemplo, los proveedores de acceso, continuarían teniendo la posibilidad de identificar una determinada dirección IP a partir de su Identificador Único, a pesar de la utilización por el usuario de la medida técnica "protectora de su anonimato". Este punto es especialmente relevante porque convertiría a este tipo de agentes tratantes en el principal medio existente para colaborar con las autoridades pertinentes en la persecución de las actividades delictivas que correspondan.

7. ¿Qué pasos se están dando con objeto de conseguir una perspectiva europea en materia de IPv6 y privacidad?

7.1. El Papel del European IPv6 Task Force

La Comisión Europea creó en el año 2001, el IPv6 Task Force ("EC IPv6 TF"), con el fin de ayudar al desarrollo del Protocolo IPv6 en Europa, siendo asimismo una de sus principales funciones atender las consultas o polémicas que pudieran surgir sobre IPv6.

Protección de datos personales

Incluso, alguno de los miembros del EC IPv6 TF son miembros del Proyecto Euro6IX, dedicados tanto a este organismo como al Proyecto de estudio del impacto de IPv6 en la intimidad.

El CE IPv6 TF entendió que la Opinión 2/2002 mencionada en otras ocasiones del Grupo del Artículo 29 potencialmente podría aportar una visión no equilibrada de los beneficios de IPv6 y, por ello, decidió convocar una reunión en el Grupo dedicado a Internet del Grupo del Artículo 29 para tratar estos asuntos con más detalle y explicar con más detenimiento los aspectos de IPv6 incidentes en materia de privacidad e intimidad.

Varios de los partners del Proyecto Euro6IX y el IPv6 Task Force formaron parte del grupo que participó en esta reunión celebrada en Bruselas, el 25 de febrero de 2003.

Con anterioridad a la celebración de esta reunión, el EC IPv6 Task Force publicó un escrito donde se trataban los siguientes aspectos:

- El EC IPv6 Task Force reconocía que el uso de identificadores únicos en cualquier tipo de tecnología o medio de comunicación (por ejemplo Ethernet, WLAN, GSM, ID Cards, IPv4 e IPv6) podría suponer un importante riesgo para la privacidad e intimidad.
- Sin embargo, el EC IPv6 Task Force puso de manifiesto que el uso de identificadores estáticos es un hecho importante para cualquier sistema de comunicación existente.
- Cualquier tipo de comunicaciones están sujetas a problemas en materia de respeto a la privacidad e intimidad y, por lo tanto, IPv6 no es ninguna excepción.
- IPv6 dispone de un mecanismo (RFC3041) que podría ayudar a resolver parte de estos problemas, mediante la aportación de un mayor grado de protección a los usuarios con respecto al facilitado por IPv4.
- Adicionalmente, los mecanismos IP Security (IPSec) se encuentran disponibles para IPv6 (RFC2460). Si bien su uso no es obligatorio en la actualidad, introducen grandes mejoras respecto a IPv4, donde actualmente IPSec no se encuentra disponible por defecto.

Las siguientes claves que se aportan deberán ser tenidas en cuenta cuando se analicen las implicaciones existentes en materia de privacidad e intimidad en cualquier sistema de comunicación basado en el protocolo IP, es decir, tanto para IPv4 como para IPv6.

1. También existen problemas en materia de privacidad e intimidad con IPv4 en relación con las direcciones fijas, ya que éstas también podrían ser consideradas como identificadores y ser rastreadas.
2. IPv6, en determinados supuestos, podrá generar direcciones IP que permitirían la correlación de actividades donde un mismo mecanismo se encuentre conectado a diferentes redes gracias a la utilización de un identificador fijo, incluido en la propia dirección IP.

Protección de datos personales

3. El RFC3041 soluciona los problemas de correlación permitiendo a una dirección IPv6, el generar un identificador aleatorio incluido en la propia dirección.
4. Muchos sistemas de Internet utilizan direcciones IP como un sistema de autenticación. Sin embargo, el respeto a la privacidad en ocasiones impide que dicha autenticación se lleve a cabo. Sin embargo, IPv6 incluye IPSec por defecto, permitiendo la utilización de sistemas más robustos de autenticación.
5. Los sistemas de extensión de IPv6 permiten que un puesto fijo, por ejemplo, el puesto de trabajo de una oficina, utilice diferentes direcciones IPv6 durante distintos momentos, por ejemplo, una dirección IPv6 distinta diariamente, permitiendo un mayor respeto a la privacidad tanto para los mecanismos no movibles como para los usuarios.
6. En IPv6 es una práctica habitual que los mecanismos que usan este protocolo tengan varias direcciones. En cambio, en IPv4, normalmente sólo existe una dirección. Será por tanto posible, en el futuro, que aplicaciones que utilicen IPv6 usen múltiples direcciones IPv6 dinámicas, lo cual reducirá, por ejemplo, la posibilidad de rastrear acciones en las aplicaciones peer to peer.
7. Investigaciones posteriores podrán incluso dar paso a la generación de nuevas clases de direcciones IPv6, por ejemplo, las generadas criptográficamente. Esto sólo será posible con IPv6.
8. El EC IPv6 TF recomendó enérgicamente que todos los proveedores y suministradores implementaran el RFC3041 por defecto en todos sus sistemas y mecanismos. De hecho, ya puso de manifiesto que alguno de ellos estaba comenzando a hacerlo.
9. En todo caso, deberían definirse sistemas sencillos para activar o desactivar el RFC3041. Incluso esta posibilidad podría hacerse de forma automática dependiendo del tráfico iniciado, encontrarse preconfigurado por defecto o incluido expresamente por solicitud del usuario. Por supuesto, esta proposición podría requerir de una labor de investigación posterior, pero en todo caso, estas posibilidades solo podrán darse gracias a IPv6".

El EC IPv6 Task Force determinó que *"el tema de la privacidad es una pieza importante en el gran ajedrez de la seguridad, transmisión, e-business, legislación aplicable e incluso un buen gobierno. Así que cualquier recomendación formulada entre distintos gobiernos sobre esta materia, sería muy útil ya que pondría de manifiesto un emergente acercamiento interdisciplinario para el futuro".*

"El EC IPv6 TF entiende que las nuevas propiedades existentes en IPv6 aportan un conjunto de herramientas para potenciar la privacidad de los usuarios de una forma que no era posible con el anterior IPv4. La combinación de IPSec junto con otras propiedades existentes en IPv6, le convierten en una herramienta muy potente para mejorar las posibilidades de protección de la privacidad de los usuarios.

Protección de datos personales

El EC IPv6 TF recomienda enérgicamente la implementación del RFC3041 por todos los suministradores y proveedores relacionados con IPv6. De todas formas, es importante tener presente que en cualquier medio de comunicación hay que mantener el equilibrio entre el respeto a la privacidad y su uso".

El EC IPv6 TF solicitó al Grupo del Artículo 29 que reconsiderara sus pronunciamientos sobre la materia teniendo en cuenta los importantes avances que IPv6 aporta en comparación con IPv4 en materia de privacidad y respeto a la intimidad. Asimismo, puso de manifiesto que un pronunciamiento de este Grupo del Artículo 29 sobre la materia tendría un impacto relevante para toda la comunidad interesada en IPv6 que tras leer su Opinión quedaron preocupados por las implicaciones de IPv6 en materia de privacidad.

7.2. Reunión con el Grupo del Artículo 29 en Bruselas, el 25 de febrero de 2003

Tras la publicación del documento analizado en el apartado anterior, el EC IPv6 TF asistió en Bruselas a la reunión mantenida con el Grupo de Internet del Artículo 29.

El IPv6 Task Force presentó su estudio e introdujo un breve análisis del RFC3041. Pretendió dejar claro una serie de puntos que deberían ser tenidos en cuenta cuando se estuvieran tratando los aspectos relativos a la privacidad tanto en IPv4 como en IPv6:

1. También existen problemas en materia de privacidad e intimidad con IPv4 en relación con las direcciones fijas, ya que éstas también podrían ser consideradas como identificadores y ser rastreadas.

2. IPv6, en determinados supuestos, podrá generar direcciones IP que permitirían la relacionar actividades, en los casos en los que un mismo mecanismo se encontrara conectado a diferentes redes, gracias a la utilización de un identificador fijo incluido en la propia dirección IP.

3. El RFC3041 podría solucionar los problemas de correlación permitiendo a una dirección IPv6, generar in identificador aleatorio incluido en la propia dirección.

Finalmente fue acordado en la reunión, de forma general, el hecho de que era necesaria la colaboración conjunta entre el EC IPv6 Task Force y el Grupo del Artículo 29 sobre este tema. El Grupo del Artículo 29 manifestó su deseo de entrar en un diálogo con el EC IPv6 Task Force e incluso se ofreció a participar en el Proyecto Euro6IX. En concreto, se ofrecieron a revisar los trabajos que sobre esta materia se iban a desarrollar a lo largo del mencionado Proyecto.

Protección de datos personales

8. Problema de la extraterritorialidad

8.1. Supuestos problemáticos

En numerosas ocasiones, resulta difícil poder determinar qué legislación, en este caso, sobre protección de datos personales, sería aplicable a un determinado tratamiento de datos, principalmente, cuando éste se efectúa en Internet.

Pensemos en una página web alojada en un determinado Estado Miembro (por ejemplo, Francia) a través de la cual se recaban datos de internautas de cualquier país del mundo y cuyo titular y, por tanto, responsable de tales ficheros, fuera una entidad con nacionalidad perteneciente a alguno de los Estados Miembros, por ejemplo, España.

El mero alojamiento de datos suele entenderse como un tratamiento de datos personales con lo que en el supuesto descrito, existirían dos agentes tratantes con distintas normativas que podrían ser de aplicación.

Si bien este supuesto conllevaría problemas de determinar la normativa aplicable, la seguridad tanto física como jurídica de los datos recabados no estaría en peligro, habida cuenta de que Estados disponen de legislación de protección de datos basada en la Directiva 95/46/CE.

Ahora pensemos en un nuevo supuesto que conllevaría mayores complicaciones: la página web se encuentra alojada a modo de hosting en Francia pero el titular de la página y responsable de tales datos pertenece a un Estado que no ha adoptado ninguna normativa de protección de datos adoptada. ¿Cómo se protegen estos datos?

8.2. Consideraciones generales a la problemática planteada

Como puede observarse, este problema trasciende al ámbito exclusivo de IPv6 puesto que es intrínseco a Internet.

Si bien es clara la tremenda dificultad de adoptar una única legislación de ámbito mundial que intente reparar este problema a través de una legislación clara y única, al menos desde la perspectiva de la Unión Europea, sería necesario continuar en la línea actual de actuación, caracterizada por la voluntad de ir creando y modelando una normativa común, férrea pero a su vez flexible, que permita solucionar, en la medida de lo posible, los mayores problemas que se deriven del tratamiento de datos de carácter personal, así como aumentar los acuerdos con distintos Estados ajenos a la UE acerca del tratamiento de datos personales, mediante labores de educación y concienciación previas.

De este modo, los Estados Miembros y aquellos con reconocidos niveles de protección deberán ir adecuando sus normativas a las iniciativas adoptadas como respuesta a los nuevos problemas surgidos en relación con el tratamiento de datos personales.

8.3. El poder de la autorregulación

Actualmente uno de los principales medios que suelen ser adoptados en el sector de Internet (junto con otros sectores) para paliar la falta de regulación específica sobre determinados temas, es la autorregulación o la adhesión a códigos de conducta elaborados por distintos sectores, a través de los cuales se incluyen una serie de normas o "buenas prácticas" que regirán las actividades de los miembros de ese sector adherido al código.

En este sentido se pronuncia la Directiva 95/46/CE cuando en su Considerando 61 establece: *"Considerando que los Estados Miembros y la Comisión, dentro de sus respectivas competencias, deben alentar a los sectores profesionales para que elaboren* ***códigos de conducta*** *a fin de facilitar, habida cuenta del carácter específico del tratamiento de datos efectuado en determinados sectores, la aplicación de la presente Directiva respetando las disposiciones nacionales adoptadas para su aplicación".*

Como puede deducirse, si bien esta opción se presenta útil, tiene un problema y es que dichos códigos no son vinculantes para aquellos agentes tratantes que no se encuentren adheridos voluntariamente a los mismos.

Algunos de los asuntos que debería contemplarse en los Códigos tipo aludidos y que sería conveniente que fueran adoptados por los citados agentes tratantes serían, entre otros, los propuestos a continuación:

- Prohibición de tratar los datos personales (incluida la dirección IP de los usuarios) para finalidades distintas de aquellas necesarias para prestar los servicios contratados por los usuarios (por ejemplo, provisión de acceso a la Red, prestación de algún servicio concreto, etc).
- Obtención del consentimiento, a través de una serie de cláusulas estándar facilitadas en los Códigos, por parte de los agentes para tratar tales datos con finalidades distintas a las de prestación de los servicios contratados (por ejemplo para la obtención de perfiles de navegación de los usuarios).
- Obtención del consentimiento de los usuarios por parte de los agentes tratantes para poder ceder datos relativos a los mismos a terceras entidades (por ejemplo obtener el consentimiento para poder ceder los datos de su dirección IP a la entidad que pudiera crearse para gestionar las guías públicas de direcciones o para remitir dichos datos a empresas de marketing dedicadas a actividades de creación de perfiles avanzados, etc).
- Determinación de una serie de medidas de seguridad que deberían aplicarse en virtud de los distintos tipos de datos que estos agentes puedan tratar en su actividad diaria, tendentes a garantizar la confidencialidad e integridad de los mismos.

En este sentido, la propia Directiva 95/46/CE ya establece esta necesidad en su Considerando 46 cuando determina *"Considerando que la protección de los derechos y libertades de los interesados en lo que respecta a los tratamientos de datos personales exige la adopción de medidas técnicas y de organización apropiadas, tanto en el momento de la concepción del sistema de tratamiento como en el de la aplicación de los tratamientos mismos, sobre todo con objeto de garantizar la seguridad e impedir, por tanto, todo tratamiento no autorizado; que corresponde a los Estados miembros velar porque los responsables del tratamiento respeten dichas medidas; que esas medidas deberán garantizar un nivel de seguridad adecuado teniendo en cuenta el estado de la técnica y el coste de su aplicación en relación con los riesgos que presente el tratamiento y con la naturaleza de los datos que deban protegerse".*

Por último, destacar que sería conveniente que este tipo de códigos fueran adoptados por los proveedores de soluciones técnicas a implementar tanto en hardware como en software, tendentes a asegurar la confidencialidad de los datos personales y la privacidad de los usuarios. De este modo, dichos proveedores quedarían informados de ciertas prácticas que deberían desarrollar en aras de proteger el derecho a la intimidad y a la protección de datos de los usuarios.

Por ejemplo, uno de los principales puntos a incluir en tales códigos sería la obligación de informar a los usuarios de la existencia de dichas medidas técnicas y de las consecuencias de su adopción o de su falta de adopción en el ámbito de la privacidad y de la protección de datos.

9. Conclusiones

A continuación, se enumeran las principales conclusiones de este estudio acerca de las implicaciones, en materia de protección de datos personales, de la utilización del nuevo Protocolo IPv6:

1. La regularización de las implicaciones en materia de protección de datos personales de IPv6 es fundamental, de manera que las entidades, organismos y los propios ciudadanos, cada vez más conscientes de sus derechos y obligaciones sobre esta materia, tengan total confianza en la seguridad y respeto de este Protocolo hacia el tratamiento de sus datos personales, puesto que sólo de este modo se garantizará su aceptación con éxito.

2. La protección de datos hace referencia a la protección jurídica de las personas en lo referente al tratamiento automatizado de los datos de carácter personal que les conciernen. En este sentido, tendrá la consideración de dato personal cualquier

información relativa a una persona identificada o identificable. Una dirección IP será un dato personal si es posible asociarla a una determinada persona física, bien de forma directa o indirectamente.

3. Con IPv6, las direcciones IP con Identificador Único permiten claramente asociar dicha IP al nodo o dispositivo que la utiliza. Entonces, si es posible que un agente tratante la asocie a su titular por algún medio, por ejemplo, a través del contrato que haya suscrito con éste o por medio del uso de guías públicas, tendrá la consideración de un dato personal y su tratamiento quedará vinculado por esta normativa.

   Si, por el contrario, el agente tratante no tuviera esta posibilidad de asociación a través de ningún medio, para él, esta dirección IP no sería un dato personal.

4. La Directiva 95/46/CE es el bloque normativo central en materia de protección de datos, a través de la cual se establecen los principios y obligaciones básicos aplicables a los tratamientos de datos personales. Sus disposiciones podrían considerarse aplicables directamente a los tratamientos de datos derivados del uso del protocolo IPv6 y, por lo tanto, puesto que las consecuencias derivadas éste no discrepan o contradicen los principios, obligaciones y derechos estipulados en la misma, cabría determinar que, en principio, no resultaría necesaria la modificación de la citada Directiva.

5. La Directiva 2002/58/CE es la regulación comunitaria que pretende regularizar las necesidades específicas en materia de protección de datos respecto de los nuevos servicios de comunicaciones electrónicas. Algunas de sus consideraciones son las siguientes:

   a. Consideración del dato de dirección IP como dato de tráfico. Cualquier tratamiento de estos datos distinto del necesario para la conducción de las comunicaciones, la facturación o como prueba de una transacción comercial, como regla general, requerirá la obtención del consentimiento del titular.

   b. La Directiva permite a los usuarios que originan llamadas, solicitar la restricción de la identificación de la línea de origen así como, a los usuarios que las reciben, impedir aquellas que provengan de líneas con identificador restringido. Por analogía, esta práctica podría ser aplicable a IPv6 y actualmente se lleva a cabo a través de soluciones técnicas basadas en el estándar RFC3041.

   c. La dirección IP puede ser considerada como un dato de localización geográfica de un determinado terminal, pudiendo existir la posibilidad de identificar, asimismo, al usuario titular del mismo.

d. Las guías públicas son uno de los medios que permitirían la asociación de una determinada IP con un determinado usuario y, por lo tanto, que potenciaría la consideración del dato de dirección IP como un dato personal. Sin embargo, es importante resaltar que la regulación ofrecida por la Directiva de las mismas, no se ajusta totalmente a la naturaleza de las guías de IP que se podrían crear, ya que la su regulación se encuentra orientada a guías telefónicas.

6. La introducción de IPv6 provoca que algunos tratamientos de información que, anteriormente, quedaban al margen de la normativa de protección de datos por incluir datos anónimos, pasen a regirse por esta normativa. En concreto, estos tratamientos serán los que se efectúen sobre el propio dato de dirección IP, en sí mismo y los que se realicen sobre la información asociada a dicho dato.

7. Uno de los principales problemas detectados con respecto a la implantación de IPv6 es la posibilidad de rastrear la navegación y actividades realizadas por el usuario conectado a la Red y asociar los resultados de dicho rastreo a un terminal y, potencialmente, a su titular o persona que los ha llevado a cabo. Estas actividades, en principio, no tendrían por qué ser consideradas ilícitas siempre y cuando el tratamiento de los datos se efectúe conforme se establece en la legislación vigente.

   En concreto, la Posición Común respecto a la elaboración de perfiles en línea en Internet, de Mayo de 2000, establece para los proveedores de servicios de Internet, la obligación de informar a los usuarios de este tipo de tratamientos y de obtener su consentimiento.

8. Las actividades de generación de perfiles, de forma inconsentida, es un problema que se viene realizando con las anteriores versiones IP y que, por lo tanto, no es un problema iniciado por el uso de IPv6. Respecto a esto, la obtención de perfiles es lícita si se efectúa dando cumplimiento a las disposiciones contenidas en la Directiva 95/46/CE y en las legislaciones de cada Estado Miembro.

9. Si la adopción del RFC3041 impidiera a ciertos agentes conocer el Identificador Único de una determinada dirección IP y asociarla al dispositivo y al titular, el dato de dirección IP, para dicho agente tratante, no tendría la consideración de dato de carácter personal y, por lo tanto, éste no quedaría obligado al cumplimiento de las obligaciones impuestas por la normativa de protección de datos personales.

   Sería recomendable que los fabricantes, tanto de software como de hardware, facilitaran a los usuarios la posibilidad de utilizar dispositivos basados en este estándar o acceder a la Red obviándolos, informándoles, a través de cláusulas informativas estandarizadas, de las posibilidades conferidas por estos mecanismos y las consecuencias de su utilización.

Protección de datos personales

10. La característica de extraterritorialidad de Internet plantea, en numerosos supuestos, problemas a la hora de determinar qué legislación debería regir ciertos tratamientos de datos personales.

11. Uno de los principales medios que suelen ser adoptados para paliar la falta de regulación específica es la autorregulación o la adhesión a códigos de conducta elaborados por distintos sectores. En este sentido, la Directiva 95/46/CE potencia la creación de los mismos por parte de los Estados Miembros, en materia de protección de datos personales.

En general, se puede afirmar que IPv6, en lo que se refiere a este documento, no es peor que IPv4 sino al contrario, proporciona medios para incrementar la intimidad de los usuarios, los cuales no están disponibles con IPv4.

Aún así, es también importante realizar un seguimiento considerando trabajos existentes y futuros relacionados con el despliegue de IPv6 (por ejemplo draft-dupont-ipv6-rfc3041harmful-04.txt), que podría implicar futuros cambios legislativos.

Derechos de Propiedad Intelectual e industrial

1. Introducción

Los avances tecnológicos producidos durante estos últimos decenios han dado lugar a la aparición de medios que posibilitan la transmisión de información en formato electrónico, en volúmenes extraordinarios, a través de redes de telecomunicaciones.

Una de las principales facetas normativas a analizar es la relativa a la protección de los contenidos transmitidos a través de redes telemáticas que se encuentran protegidos por el ámbito normativo sobre Propiedad Intelectual.

Sin embargo, no toda la información transmitida por medios electrónicos, por ejemplo a través de Internet, es susceptible de ser protegida por Propiedad Intelectual, pero sí es importante resaltar que, aún así, el volumen de contenidos protegibles es considerablemente grande. Aún más, el ya referido aumento de los volúmenes de información transmitida, por las nuevas mejoras tecnológicas como, por ejemplo, IPv6, supone el correlativo aumento de contenidos susceptibles de ser protegidos por la normativa sobre Propiedad Intelectual.

Sobre la base de este contexto, los objetivos de este Capítulo se centran en el análisis de las posibles relaciones que cabe establecer entre el desarrollo de IPv6 y la normativa sobre Propiedad Intelectual o, más concretamente, las características del nuevo Protocolo que puedan ser útiles a los efectos de procurar o mejorar la protección de los Derechos de Propiedad Intelectual (DPI).

No es desconocido que el Protocolo IPv6 no tiene como objetivo propio la protección de estos derechos ni la generación de fórmulas destinadas a este fin. Por ello, el análisis que se realice del propio Protocolo, de la normativa aplicable, de los problemas actuales sobre transmisión de contenidos en Internet, etc. se debería realizar bajo la perspectiva de determinar qué características de IPv6 podrían extender su uso hacia la protección de los DPI y, por tanto, hacia la mejora en la gestión de contenidos en el ámbito electrónico, donde IPv6 va a jugar un papel fundamental.

Es necesario insistir en que, en último término, cualesquiera conclusiones que se extraigan de este Capítulo, en cuanto a la protección de los citados derechos, se aplicarán únicamente sobre aquella parte de los datos transmitidos por redes de comunicación, haciendo uso del nuevo Protocolo, que sean susceptibles de protección por la normativa sobre Propiedad Intelectual.

Con este fin, se realiza, en una primera parte del Capítulo, un acercamiento al concepto de Propiedad Intelectual y recoge las características principales de los objetos susceptibles de DPI (patentes, marcas, dibujos y diseños industriales y derechos de autor), siempre focalizando la atención sobre aquellas características que sean más interesantes con relación a los objetivos que se pretenden en el libro.

Derechos de Propiedad Intelectual e industrial

Una vez establecidos estos conceptos, seguidamente, se señalarán las principales referencias normativas sobre Propiedad Intelectual en la Unión Europea, con el fin de establecer los aspectos más importantes de la relación entre IPv6 y Propiedad Intelectual que se recogen en el marco jurídico comunitario.

A continuación, se analizan en los principales retos y problemas a los que se enfrenta la Propiedad Intelectual dentro del ámbito electrónico y las líneas fundamentales de influencia que podría tener el nuevo Protocolo IPv6 en el ámbito de los DPI, intentando profundizar en aquellos elementos del Protocolo que pudieran ser útiles a los fines de protección de los derechos citados.

Como consecuencia de lo anterior, se extrae la consideración de que una de las características principales de IPv6 a efectos de protección de los DPI podría encontrarse en el Protocolo de seguridad IPSec, ya utilizado actualmente de manera conjunta con la versión 4 del Protocolo (IPv4), pero que con el nuevo Protocolo va a adquirir características reforzadas y, sobre todo, va a configurarse como un elemento intrínseco al mismo. Por ello, se trata de establecer cómo estas características de seguridad, relativas a las transmisiones de información, podrían aprovecharse para mejorar la protección y gestión de los contenidos susceptibles de DPI.

2. La Propiedad Intelectual

2.1. Concepto

El estudio de las consecuencias normativas de la circulación de contenidos protegibles por DPI por las redes telemáticas, públicas o privadas, no sólo se hace necesario para tratar las peculiaridades que puede conllevar el propio medio de transmisión y la utilización del nuevo Protocolo IPv6, sino que, además, es interesante desde una doble perspectiva:

- Las nuevas formas de violación de DPI que se han generado como consecuencia de las posibilidades técnicas tanto de supresión de las barreras tecnológicas de protección de derechos como de las grandes posibilidades de transmisión de la información entre los intervinientes en las comunicaciones electrónicas.
- La necesidad de disponer de una normativa ágil y flexible que permita asegurar la protección de los DPI, intentando, incluso, crear un marco regulatorio que no sólo focalice su atención sobre los medios electrónicos de explotación ya existentes, sino que sea capaz de asumir la regulación de los que puedan surgir en el futuro como consecuencia del incesante crecimiento de las nuevas tecnologías.

No obstante, antes de seguir, se ha de establecer a qué nos estamos refiriendo con el concepto “Propiedad Intelectual”, ya que se trata de un área jurídica de gran amplitud

Derechos de Propiedad Intelectual e industrial

de la cual se deben extraer aquellos elementos o partes que sean de verdadero interés a los efectos del presente Capítulo.

La Propiedad Intelectual tiene que ver con las creaciones de la mente, tales como, por ejemplo: las invenciones, las obras literarias y artísticas, los símbolos, la música, las imágenes y obras audiovisuales y los dibujos y modelos utilizados en el comercio(2).

Las categorías en que se divide la Propiedad Intelectual en el ámbito comunitario, con independencia de que en las legislaciones de algunos países miembros (por ejemplo España) se estructure de modo diferente, serían, siguiendo lo establecido por la Organización Mundial de la Propiedad Intelectual (OMPI), las siguientes:

- La Propiedad Industrial, que incluye patentes, marcas, dibujos y modelos industriales e indicaciones geográficas.
- El derecho de autor, que abarca las obras literarias tales como las novelas, los poemas y las obras de teatro, las películas, las obras musicales y las obras artísticas tales como los dibujos, pinturas, fotografías, esculturas y los diseños arquitectónicos(3).

Asimismo, los derechos conexos, son los derechos de los artistas intérpretes o ejecutantes sobre sus interpretaciones o ejecuciones, los derechos de los productores de fonogramas sobre sus grabaciones y los derechos de los organismos de radiodifusión sobre sus programas de radio y de televisión(4).

Antes de comenzar la parte del Capítulo en la que se recogen las notas principales de cada uno de los objetos protegidos por Propiedad Intelectual, siempre bajo la perspectiva de detectar los elementos más interesantes con relación al Protocolo IPv6, se debe incidir en la idea de que no toda información, dato, archivo, etc. que circula por una red telemática, por ejemplo, Internet, es susceptible de DPI. Por tanto, las consideraciones que se realicen con relación a la influencia de IPv6 en la protección de DPI se refieren sólo a aquellos contenidos transmitidos por redes telemáticas que son susceptibles de la aplicación de tales derechos, por ejemplo, música, películas, fotografía, obras literarias, software, etc.

2.2. Descripción de los objetos protegidos

El presente subapartado tiene como fin establecer, de forma resumida, las notas descriptoras de cada una de las categorías de elementos protegibles, focalizando la atención sobre aquellas que pudieran resultar de mayor interés a los efectos del presente Capítulo, es decir, aquellas que, de una u otra manera, pudieran ser útiles en la configuración del papel que IPv6 puede tener en la protección de los DPI e, incluso, en su mejor gestión, en el ámbito electrónico.

(2), (3) y (4) http://www.wipo.org

Derechos de Propiedad Intelectual e industrial

2.2.1. Patentes

Una patente es un derecho exclusivo concedido a una invención, que es el producto o proceso que ofrece una nueva manera de realizar un producto o prestar un servicio o un desarrollo novedoso en cuanto a la forma de realización o de prestación ya existentes.

Una patente proporciona protección al titular de la invención, la cual se concede durante un periodo limitado de tiempo, que suele ser de 20 años.

Además, los detalles de la invención deben ser publicados. Esto significa que, a pesar de que la concesión de la patente revierta en el inventor, el desarrollo tecnológico se difunde a partir del momento en que los detalles de la patente se hacen públicos y pueden ser explotados por terceras partes, después de que el derecho de patente haya expirado.

Es importante resaltar que solo ciertos tipos de innovaciones son patentables. En concreto, las invenciones (es decir, productos o procesos) calificables como novedosas, en cuanto que no sean obvias para una persona conocedora o familiarizada con la tecnología o arte relacionado con la nueva patente. No es posible patentar lo que ya se conoce.

Desde un punto de vista jurídico, la protección de una patente significa que la invención no puede ser confeccionada, utilizada, distribuida, vendida comercialmente, etc. sin el consentimiento del titular de la patente. Es decir, es el titular de una patente quien tiene el derecho de decidir quién puede o no puede utilizar la invención patentada durante el periodo en el que está protegida la invención.

No obstante, el titular de la patente puede articular formas de utilización de la invención por terceros, a través de licencias, cuyas condiciones se establecerán de común acuerdo entre el titular de la patente y el licenciatario. Incluso, el titular puede transmitir a un tercero su derecho a la invención, por ejemplo, mediante compraventa. En este caso, el tercero adquirirá la condición de titular de la patente.

Por último, es importante que cuando la patente expira, lo hace asimismo la protección, lo que da lugar a que la invención pase a pertenecer al dominio público. Es decir, el titular deja de detentar derechos exclusivos sobre la invención, que pasa a estar disponible para la explotación comercial por parte de terceros.

2.2.2. Marcas

Una marca es un signo distintivo, susceptible de representación gráfica, que indica que ciertos bienes han sido producidos o ciertos servicios han sido prestados por una persona o empresa determinada.

Las marcas pueden consistir en una palabra o en una combinación de palabras, letras y cifras. Pueden consistir, asimismo, en dibujos, símbolos, rasgos en tres dimensiones, signos auditivos, colores u otros elementos que sean utilizados como características distintivas.

De esta manera, una marca ofrece protección al titular de la marca, garantizándole el derecho exclusivo a utilizarla para identificar sus bienes o servicios o a autorizar a un tercero a utilizarla a cambio de pago.

Uno de los objetivos fundamentales del sistema de marcas es obstaculizar los esfuerzos de los competidores desleales como, por ejemplo, los falsificadores, destinados a utilizar signos distintivos similares para designar productos o servicios distintos a los amparados por una marca y, en muchas ocasiones, de calidad inferior. En el ámbito electrónico, en el que va a cobrar tanta importancia IPv6, el sistema de marcas sirve, entre otros fines, para obstaculizar y perseguir la utilización ilegítima de signos distintivos o marcas por terceras partes no autorizadas para ello, lo cual supondría un infracción de los DPI (por ejemplo nombres de dominio, utilización de logos sin autorización en sitios web, venta a través del canal Internet de productos falsificados, etc.).

Además de las marcas que identifican el origen comercial de bienes y servicios, existen otras categorías de marcas. Así, por ejemplo, existen las marcas colectivas, que son propiedad de una asociación cuyos miembros las utilizan para identificar que cuentan con un nivel de calidad determinado y con otros requisitos establecidos por la asociación. Por otro lado, las marcas de certificación se conceden a un producto que satisface determinadas normas, pero no se restringen a los miembros de organizaciones. Pueden ser concedidas a cualquiera que pueda certificar que los productos en cuestión satisfacen ciertos estándares establecidas (por ejemplo ISO 9001).

2.2.3. Dibujos y modelos industriales

Un dibujo o modelo industrial puede definirse como el aspecto ornamental o estético de un artículo. El dibujo o modelo industrial puede consistir en rasgos en tres dimensiones, como la forma o la superficie de un artículo, o rasgos en dos dimensiones, como los diseños, las líneas y el color.

Un dibujo o modelo industrial debe ser no funcional, es decir, que debe tener un carácter esencialmente estético, ya que la legislación no protege ninguno de los rasgos técnicos del artículo al que se aplica.

El sistema de protección de los dibujos o modelos industriales proporciona al titular de los mismos (la persona o entidad que ha registrado un dibujo o modelo industrial), el derecho exclusivo contra la copia no autorizada o la imitación del dibujo o modelo industrial por parte de terceros.

2.2.4. Derechos de autor

El derecho de autor es un término jurídico que describe los derechos concedidos a los creadores por sus obras literarias y artísticas.

Derechos de Propiedad Intelectual e industrial

El tipo de obras protegibles por derecho de autor son las siguientes: obras literarias como novelas, poemas, obras de teatro, documentos de referencia, periódicos, programas informáticos, bases de datos, películas, composiciones musicales, coreografías; obras artísticas como pinturas, dibujos, fotografías y esculturas, obras arquitectónicas, publicidad, mapas y dibujos técnicos.

La importante evolución de las comunicaciones telemáticas y de la Sociedad de la Información ha supuesto un planteamiento de nuevas vías de explotación de los contenidos protegidos por derechos de autor pero también ha conllevado nuevos y graves problemas derivados de la mayor facilidad en el ámbito electrónico para la violación de estos derechos de autor.

Como ya se ha dicho, la evolución tecnológica de los medios de transmisión de información en el ámbito electrónico, permite, cada vez con mayor facilidad, el envío y recepción de gigantescas cantidades de información. Y, en muchas ocasiones, los datos o informaciones transmitidos incluyen, en mayor o menor medida, contenidos susceptibles de DPI. Aún más, el desarrollo de Protocolos como IPv6 van a posibilitar el aumento de las capacidades y facilidades de transmisión. Es por ello que, en el desarrollo del Protocolo, se deben plantear qué características del mismo son o pueden ser útiles con el fin de establecer, reforzar o mejorar el sistema de protección de DPI y buscar el adecuado equilibrio entre la mejora y optimización de las transmisiones de contenidos y el respeto de los DPI.

Volviendo a las características definitorias de los derechos de autor, cabe señalar que los creadores originales de obras protegidas, así como sus herederos, gozan de ciertos derechos básicos. Entre ellos, detentan el derecho exclusivo de utilizar la obra o autorizar a terceros a que la utilicen en condiciones convenidas de común acuerdo. Asimismo, el creador de una obra puede prohibir o autorizar:

- Su reproducción bajo distintas formas.
- Su interpretación o ejecución pública.
- Su grabación.
- Su transmisión.
- Su traducción a otros idiomas o su adaptación.

Con más detalle, el derecho de autor se concreta, principalmente, en el ejercicio exclusivo por el mismo de los denominados derechos patrimoniales o de explotación de su obra en cualquier forma. Los principales derechos patrimoniales o de explotación son:

- Derecho de reproducción, en el sentido de fijación de la obra en un medio que permita su comunicación y la obtención de copias de toda o parte de ella.

Derechos de Propiedad Intelectual e industrial

- Derecho distribución, que hace referencia a la puesta a disposición pública del original o copias de la obra mediante su venta, alquiler, préstamo o de cualquier otra forma legítima.
- Derecho a la comunicación pública, entendida como todo acto por el cual una pluralidad de personas pueda tener acceso a la obra sin previa distribución de ejemplares a cada una de ellas.
- Derecho de transformación, que comprende la traducción de la obra, su adaptación y cualquier otra modificación en su forma de la que derive una obra diferente.

Como es fácilmente constatable, todos y cada uno de estos derechos se manifiestan de modo cada vez más frecuente en el ámbito de las comunicaciones electrónicas y, como ejemplo más conocido, en Internet. Incluso, la transmisión de contenidos susceptibles de estos derechos va a ser cada vez más importante y de mayor volumen, por el avance de desarrollos tecnológicos como IPv6. La transmisión de vídeo y audio en tiempo real, las posibilidades de intercambio de ficheros, vídeo bajo demanda en Internet, etc. son meros ejemplos que reflejan la necesidad de buscar qué elementos del aspecto técnico, por ejemplo, el Protocolo IPv6, son oportunos para la protección de los derechos, por ejemplo teniendo en cuenta las utilidades que, a este fin, pudieran tener los modos de direccionamiento (multicast, unicast y anycast) del Protocolo.

Por otro lado, la protección por derecho de autor también incluye los denominados derechos morales, que equivalen al derecho a reivindicar la autoría de una obra y al derecho a oponerse a modificaciones de la misma que puedan atentar contra la reputación del creador.

Un principio de base en materia de derechos de autor es que éstos protegen únicamente las expresiones pero no las ideas, procedimientos, métodos de operaciones o conceptos matemáticos en sí.

En torno a las obras protegidas por el derecho de autor, han ido desarrollándose los denominados derechos conexos. Mediante los mismos, se conceden derechos similares, aunque a menudo más limitados y de más corta duración, a los derechos de autor. La concesión se realiza a:

- Los artistas intérpretes o ejecutantes respecto de sus interpretaciones o ejecuciones.
- Los productores de grabaciones sonoras respecto de sus grabaciones.
- Los organismos de radiodifusión respeto de sus programas de radio y de televisión.

Asimismo, en el ámbito de los derechos de autor es necesario hacer referencia al concepto de Gestión Colectiva del derecho de autor y de los derechos conexos. Esta figura surge de la evidente imposibilidad de muchos autores de llevar a cabo una gestión individual

de los derechos patrimoniales sobre las obras de las que son titulares. Por ello surge el concepto de Gestión Colectiva, como el ejercicio del derecho de autor y los derechos conexos por intermedio de organizaciones que actúan en representación de los titulares de derechos, en defensa de sus intereses.

Por lo general, las organizaciones de Gestión Colectiva se ocupan de los siguientes derechos:

- El derecho de representación y ejecución pública.
- El derecho de radiodifusión.
- Los derechos de reproducción mecánica sobre las obras musicales.
- Los derechos de representación y ejecución sobre las obras dramáticas.
- El derecho de reproducción reprográfica sobre las obras literarias y musicales.
- Los derechos conexos.

Por último, destacar que el derecho de autor y los derechos conexos son esenciales para la creatividad humana al ofrecer a los autores incentivos en forma de reconocimiento y recompensas económicas equitativas. Este sistema de derechos garantiza a los creadores la divulgación de sus obras sin temor a que se realicen copias no autorizadas o actos de piratería. A su vez, ello contribuye a facilitar el acceso y a intensificar el disfrute de la cultura, los conocimientos y el entretenimiento en todo el mundo.

3. La legislación sobre propiedad intelectual en la Unión Europea: Principales Referencias

3.1. Directivas comunitarias

3.1.1. Directiva 2001/29/CE, armonización de los derechos de autor y derechos conexos en la Sociedad de la Información

Con el objetivo de adaptar la legislación relativa a derecho de autor y derechos conexos a los cambios tecnológicos y especialmente a la denominada Sociedad de la Información, se promulgó la Directiva 2001/29/CE, del Parlamento Europeo y del Consejo, de 22 de mayo de 2001, relativa a la armonización de determinados aspectos de los derechos de autor y derechos conexos a los derechos de autor en la Sociedad de la Información (Directiva 2001/29/CE).

Adicionalmente, la Directiva 2001/29/CE tiene como objetivo transponer en el ámbito comunitario las principales obligaciones internacionales derivadas de los dos Tratados sobre los derechos de autor y derechos conexos aprobados por Organización Mundial

Derechos de Propiedad Intelectual e industrial

de la Propiedad Intelectual (OMPI) en 1996:

- Tratado de la OMPI sobre Derecho de Autor
- Tratado de la OMPI sobre Interpretación o Ejecución y Fonogramas

La existencia de este objetivo de transposición o adaptación de la normativa de los países comunitarios a los citados Tratados de la OMPI, hace conveniente que se recojan en este Capítulo sus criterios más relevantes a los efectos de determinar los principales puntos a tener en cuenta sobre esta materia y sus posibles implicaciones respecto de la implantación del nuevo Protocolo IPv6.

Por lo que respecta al Tratado de la OMPI sobre Derecho de Autor y siempre resaltando los aspectos más relevantes para el objeto de estudio del bloque, cabe destacar que:

- Los países que pretendan el cumplimiento del Tratado deberán establecer la protección jurídica adecuada y los recursos jurídicos efectivos para evitar toda acción que pretenda eludir las medidas tecnológicas utilizadas por los autores respecto de sus obras, a fin de ofrecerles la protección correspondiente otorgada por este Tratado o por el Convenio de Berna para la Protección de las Obras Literarias y Artísticas.
- Además, se deberán proporcionar recursos jurídicos efectivos para poder dirigirse contra cualquier persona que, con conocimiento de causa, realice determinados actos que induzcan, permitan, faciliten u oculten una infracción de cualquiera de los derechos previstos en el propio Tratado o en el citado Convenio de Berna. En concreto, los actos vulneradores podrán ser:

  a. Suprimir o alterar, sin autorización, cualquier información electrónica sobre la gestión de derechos. De conformidad con el Tratado, se debe entender por "información sobre la gestión de derechos", la información que identifica a la obra, al autor, al titular de cualquier derecho sobre la obra, o información sobre los términos y condiciones de utilización de la obra, y todo número o código que represente tal información, cuando cualquiera de estos elementos estén adjuntos a un ejemplar de una obra o figuren en relación con la comunicación al público de ésta.

  b. Distribuir, importar para su distribución, emitir o comunicar al público, sin autorización, ejemplares de obras sabiendo que la información electrónica sobre la gestión de derechos ha sido suprimida o alterada sin autorización.

Por lo que respecta al Tratado OMPI sobre Interpretación o Ejecución y Fonogramas, se debe indicar que los aspectos más destacables del mismo, a los efectos del presente bloque, coinciden, prácticamente en su totalidad, con los señalados respecto del Tratado OMPI sobre Derecho de Autor. En concreto, se establece que:

- Con relación a las medidas tecnológicas que artistas intérpretes o ejecutantes o productores de fonogramas pretendan establecer para el respeto de sus derechos, los países que quieran cumplir con el Tratado, deberán proporcionar protección jurídica adecuada y recursos jurídicos efectivos contra las acciones de elusión de dichas medidas.

- Además, se deberán proporcionar recursos jurídicos adecuados y efectivos contra cualquier persona que, con conocimiento de causa, realice actos que infrinjan estos derechos o respecto de la cual existan motivos razonables para saber que induce, permite, facilita u oculta una infracción de cualquiera de los derechos previstos en el Tratado. En concreto, los actos vulneradores podrán ser la supresión o alteración, sin autorización, de cualquier información electrónica sobre la gestión de derechos o la distribución, emisión, comunicación o puesta a disposición del público, sin autorización, de interpretaciones o ejecuciones, ejemplares de interpretaciones o ejecuciones fijadas o fonogramas.

Volviendo a la Directiva 2001/29/CE, los contenidos regulatorios de mayor interés, a los efectos del presente Capítulo, coinciden, en gran medida, con los expresados en los Tratados OMPI.

Es interesante como ya en el Considerando (55) de la norma y con relación a las informaciones que ayuden a la gestión de derechos, se viene a indicar que:

- La mayor facilidad para la distribución de obras que procuran los avances tecnológicos, conlleva, para los titulares de las obras distribuidas, la necesidad de identificar mejor la obra o la prestación, el autor o el titular del derecho y, además, proporcionar información sobre las condiciones y modalidades de utilización de la obra o prestación, con objeto de simplificar la gestión de derechos.

- Incluso, se indica que debe "alentarse" a los titulares de los derechos a emplear "marcados" que indiquen, además de la información sobre gestión de derechos, entre otras cosas, la autorización adecuada cuando se incluyan en redes telemáticas las obras o prestaciones protegidas.

- Es necesario establecer una protección jurídica, armonizada a nivel comunitario, tendente a evitar actividades destinadas suprimir o alterar la información para la gestión electrónica de los derechos de autor vinculada a la obra.

Entrando en el articulado de la Directiva 2001/29/CE, el artículo 6 se dedica a las "Obligaciones relativas a medidas tecnológicas", el cual, de manera resumida, indica que:

- Se establecerá una protección jurídica adecuada contra la elusión de cualquier medida tecnológica efectiva adoptada para la protección de derechos de autor.

Derechos de Propiedad Intelectual e industrial

- Se establecerá una protección jurídica adecuada frente a la fabricación, importación, distribución, venta, alquiler, publicidad para la venta o alquiler, o posesión con fines comerciales, de cualquier dispositivo, producto o componente o la prestación de servicios que:

  a. Sea objeto de una promoción, publicidad o comercialización con la finalidad de eludir la medida tecnológica.

  b. Sólo tenga una finalidad o uso comercial limitado al margen de la elusión de la medida tecnológica.

  c. Esté principalmente concebido, producido, adaptado o realizado con la finalidad de permitir o facilitar la elusión de la medida tecnológica.

- Se define como "medidas tecnológicas" toda técnica, dispositivo o componente que, en su funcionamiento normal, esté destinado a impedir o restringir actos referidos a obras o prestaciones protegidas, que no cuenten con la autorización del titular de los derechos de autor o de los derechos conexos. Las medidas tecnológicas se consideran "eficaces" cuando el uso de la obra o prestación protegidas esté controlado por los titulares de los derechos mediante la aplicación de un control de acceso o un procedimiento de protección, por ejemplo, codificación, aleatorización u otra transformación de la obra o un mecanismo de control de copiado, que logre este objetivo de protección.

Por su parte, el artículo 7 establece las normas con respecto a las "Obligaciones relativas a la información para la gestión de derechos". De manera resumida, este artículo viene a determinar que:

- Se deberá establecer una protección jurídica adecuada frente a todas aquellas personas que, a sabiendas, lleven a cabo, sin autorización, determinados actos, sabiendo o teniendo motivos razonables para saber que al hacerlo inducen, permiten, facilitan o encubren una violación de los derechos de autor o de los derechos conexos. En concreto, los actos vulneradores serían similares a los determinados en momentos anteriores de este Capítulo.

- Se define la "información para la gestión de derechos" como toda información facilitada por los titulares de los derechos que identifique la obra o prestación protegida, al autor o cualquier otro derechohabiente, o información sobre las condiciones de utilización de la obra o prestación protegida, así como cualesquiera números o códigos que representen dicha información.

Derechos de Propiedad Intelectual e industrial

3.1.2. Directiva 2004/48/CE, respeto de los Derechos de Propiedad Intelectual

La Directiva 2004/48/CE, de 29 de abril, relativa al respeto de los DPI, se promulga con el fin de lograr, en el ámbito de la Unión Europea, otros objetivos adicionales como son:

- Impedir las pérdidas, fiscales y para las propias empresas, que produce la piratería. Estas pérdidas pueden suponer, incluso, un factor de desestabilización de los mercados ya que, por ejemplo, en el caso de los productos multimedia, la usurpación de marca y la piratería por Internet no dejan de aumentar y ocasionar, en consecuencia, pérdidas muy sustanciales.
- Velar por la protección de los consumidores, en cuanto que la usurpación de marca y la piratería suelen ir acompañadas de un engaño deliberado al consumidor sobre la calidad que tiene derecho a esperar de un producto concreto.

Partiendo desde un punto de vista general, con estos objetivos, los Considerandos de la norma que pueden resultar de mayor interés a los efectos del presente Capítulo, serían:

- El Considerando (2) indica que, aunque la Propiedad Intelectual debe permitir que el inventor o creador obtenga un beneficio legítimo de su invención o creación, así como permitir la difusión más amplia posible de obras, ideas y nuevos conocimientos, ello no puede ser obstáculo para la libre circulación de la información, inclusive en Internet.

  En definitiva, se viene a plantear la necesidad de conseguir un equilibrio entre la protección de los derechos de los autores de los contenidos transmitidos y el derecho a que la información, incluidos esos contenidos, circule libremente. Si bien lograr este equilibrio resulta sencillo desde un punto de vista teórico, en la práctica y con la existencia de medios de difusión tan potentes como aquellos sobre los que se sustenta Internet, se plantean serias dificultades a la hora de controlar la protección de los derechos de autor, por ejemplo, con los masivos intercambios de música o vídeo a través del aplicaciones P2P. Es en este contexto donde se plantean los objetivos del bloque en cuanto establecer en qué medida IPv6 puede ayudar a "combatir" las actividades contrarias a la Propiedad Intelectual, por ejemplo, la piratería.
- El Considerando (14) define los denominados "actos llevados a cabo a escala comercial" como aquellos realizados para obtener beneficios económicos o comerciales directos o indirectos, excluyéndose, normalmente, los actos realizados por los consumidores finales de buena fe.
- El Considerando (20) refleja la importancia de la prueba como elemento fundamental para la comprobación de la comisión de la infracción de los DPI, indicando que conviene garantizar que se pongan de manera efectiva a disposición de las partes medios de presentación, obtención y protección de pruebas.

Derechos de Propiedad Intelectual e industrial

- El Considerando (21) describe el Derecho de información como aquel que permite obtener datos precisos sobre el origen de las mercancías o servicios litigiosos, los circuitos de distribución y la identidad de cualesquiera terceras personas implicadas en la infracción.

Entrando ya en el articulado de la norma, es relevante señalar que, el artículo 1 de la misma, indica que, a los fines de la propia Directiva, el término DPI incluirá los derechos de Propiedad Industrial.

Por su parte, los artículos 6 a 8, relativos a "Pruebas" indican, de manera resumida, que:

- Sin perjuicio de los datos confidenciales, en el caso de que la parte que haya presentado pruebas razonablemente disponibles y suficientes para respaldar sus alegaciones, haya especificado, al fundamentar sus alegaciones, qué otras pruebas se encuentran bajo control de la parte contraria, las autoridades judiciales competentes pueden ordenar que la parte contraria entregue dichas pruebas.
- A instancia de partes que hayan presentado pruebas razonablemente disponibles para respaldar sus alegaciones, se podrían dictar medidas rápidas y eficaces para proteger pruebas pertinentes con respecto a la supuesta infracción, sin perjuicio, de nuevo, de que sea necesario garantizar la protección de toda información confidencial.

En este sentido, IPv6, técnicamente, provee de medios de prueba más precisos que los aportados por su versión anterior, IPv4, por ejemplo, en la manera de identificar a los intervinientes en una transmisión de información o en la trazabilidad de las comunicaciones.

En cuanto al derecho de información, el artículo 8 de la Directiva indica que, en el contexto de los procedimientos relativos a una infracción de un DPI y en respuesta a una petición justificada y proporcionada del demandante, las autoridades judiciales competentes pueden ordenar que se faciliten datos sobre el origen y las redes de distribución de las mercancías o servicios que infringen un DPI, sobre el infractor o sobre cualquier persona que haya sido hallada en posesión de las mercancías litigiosas o utilizando servicios litigiosos, en ambos casos, a escala comercial.

En relación con este punto, comienza a ser frecuente que en la legislación nacional de algunos Estados Miembros se contemple un deber de retención de datos de tráfico en el ámbito de las comunicaciones electrónicas, por ejemplo, los datos relativos a las IP´s intervinientes en una comunicación, logs, datos transaccionales, etc., lo que, por un lado, posibilita el mejor cumplimiento de lo exigido por el citado artículo 8 de la Directiva, así como se convierte en un medio para hacer más efectiva la persecución de vulneraciones de los DPI´s.

Derechos de Propiedad Intelectual e industrial

3.2. Reglamento sobre la marca comunitaria

La norma fundamental en Derecho comunitario sobre la regulación de las marcas, es el Reglamento (CE) nº 40/94 del Consejo, de 20 de diciembre de 1993, sobre la marca comunitaria, con el que se pretendía crear una marca que pudiera aplicarse en todo el ámbito comunitario.

Sobre esta base normativa, se establece un sistema que permite la concesión de marcas comunitarias por la denominada Oficina de Armonización del Mercado Interior. A través de una solicitud única presentada ante la OAMI, la marca comunitaria tiene carácter unitario, en el sentido de que produce los mismos efectos en el conjunto de la Comunidad Europea.

Podrán constituir marcas comunitarias todas las señales que puedan ser objeto de representación gráfica, siempre que tales señales permitan distinguir los productos o servicios de una empresa de los de otras empresas.,

La marca comunitaria confiere a su titular un derecho exclusivo, de tal manera que el titular tiene derecho a prohibir a un tercero usar con fines comerciales:

- Una señal idéntica a la marca comunitaria para productos o servicios idénticos a aquellos para los que se registró la marca.
- Una señal para la cual existe riesgo de confusión, en el espíritu del público, con otra marca.
- Una señal idéntica o similar a la marca comunitaria para productos o servicios que no sean similares a aquellos para los cuales se registra la marca comunitaria, cuando el uso de la señal saque provecho del prestigio o del carácter distintivo de la marca.

En cambio, el derecho conferido por la marca comunitaria no permite a su titular prohibir a un tercero el uso, con fines comerciales de:

- Su nombre o dirección.
- Indicaciones relativas a la especie, a la calidad, a la cantidad, al destino, al valor, a la procedencia geográfica, a la época de fabricación del producto o de la prestación del servio o a otras características de éstos.
- La marca, cuando este uso sea necesario para indicar el destino de un producto o de un servicio, en particular, como accesorio o repuesto.

3.3. Propuesta de Reglamento sobre patente comunitaria

Con el objetivo, entre otros, de crear un nuevo título unitario de Propiedad Industrial para eliminar los obstáculos a la libre circulación de mercancías en el mercado interior, se ha redactado la Propuesta de la Comisión, de 1 de agosto de 2000, de Reglamento del Consejo sobre la patente comunitaria.

Actualmente, existen en el ámbito de la UE dos formas de garantizar la protección mediante patente: los sistemas nacionales de patentes y el sistema europeo de patentes, articulado a través del Convenio, de 5 de octubre de 1973, de concesión de patentes europeas, conocido como Convenio de Munich.

A pesar de que el Convenio de Munich crea un sistema único de concesión de patentes, no existe todavía una patente comunitaria que forme parte del ordenamiento jurídico comunitario.

El objeto de la Propuesta de Reglamento sobre patente comunitaria no es sustituir los actuales sistemas nacionales y el sistema europeo, sino añadirse a ellos, por lo que deberán ser los solicitantes quienes elijan la opción que deseen.

No obstante, la idea principal de la Propuesta es que el Reglamento complete el Convenio de Munich. Así, por ejemplo, las condiciones de concesión de la patente están fijadas mediante el Convenio de Munich.

La patente comunitaria conferirá a su titular el derecho de prohibir a cualquier tercero que no tenga su consentimiento:

- La explotación directa de la invención y, en concreto, fabricarla, ofrecerla, introducirla en el mercado, importarla, etc.
- La explotación indirecta de la invención.

La utilización de la patente por persona diferente a su titular se articula a través de un sistema de licencias, las cuales, incluso, pueden llegar a ser obligatorias, por ejemplo, por falta o insuficiencia de explotación de la patente comunitaria.

4. Situación de los Derechos de la Propiedad Intelectual

Una vez analizados algunos de los aspectos más relevantes de la normativa comunitaria en materia de Propiedad Intelectual, el bloque se centra, en este apartado, en reflejar cuáles son las principales problemáticas existentes en esta materia en el ámbito de las comunicaciones electrónicas e Internet.

Derechos de Propiedad Intelectual e industrial

El gran desarrollo de las redes electrónicas de transmisión de la información, siendo Internet y el correo electrónico las expresiones más difundidas de este fenómeno, y el desarrollo de los soportes electrónicos de datos en sus diversas variantes, han provocado, por un lado, nuevas vías de explotación de los DPI y, por otro lado, el efecto pernicioso de dar lugar a un vertiginoso aumento de los medios de violación de los mismos.

Con objeto de tratar las principales vulneraciones de DPI que se producen actualmente en el ámbito electrónico para posteriormente, poder analizar si el uso del Protocolo IPv6 puede ser un medio para provocar la desaparición o minimización de todos o alguno de ellos, se ha de centrar la atención en los dos tipos de derechos más frecuentemente vulnerados: los Derechos de Autor y los Derechos de Marca.

En cuanto a los Derechos de Autor, las formas de vulneración de los mismos mediante medios electrónicos son de sobra conocidas. Como mero ejemplo se pueden reseñar las siguientes:

- Intercambio de ficheros en redes P2P sin permiso de los autores y sin abono de las retribuciones que corresponderían.
- Promoción, distribución y utilización de técnicas de supresión o deshabilitación de los sistemas anticopia de determinados ficheros, incorporados o no en un soporte informático.
- Piratería de música, software, juegos, y, en general, contenidos protegibles por Propiedad Intelectual, bien por su venta, alquiler, etc. a través de Internet o bien por su incorporación a un soporte informático.
- Apropiación de contenidos (texto, fotos, archivos audiovisuales, etc.) publicados en Internet sin licencia de sus autores o excediendo la licencia concedida.

Con relación al Derecho de Marcas, entre los principales ejemplos de violación de los mismos a través de medios electrónicos se pueden citar los siguientes:

- Vulneración a través de prácticas que, en muchos casos, suponen, además, supuestos de competencia desleal, como ocurre, en ocasiones, con los contenidos de ciertos envíos indiscriminados de mensajes de correo electrónico no solicitado o spam.
- Phishing, técnica que consiste en atraer mediante engaño a un usuario hacia un sitio web fraudulento donde se le insta a introducir datos privados. En el común de los casos, el sitio web fraudulento utiliza objetos susceptibles de derecho de marca, titularidad de la empresa o entidad que se pretenda simular.
- Spoofing, técnica tendente a simular o usurpar la identidad de un elemento de red (ordenador personal, servidor, router, etc.), cuya identidad se habría obtenido anteriormente, para conseguir acceso a los recursos de un tercer sistema, acceso que se basa en la confianza que el sistema accedido tiene en el elemento de red suplantado.

Lógicamente, las técnicas de averiguación y suplantación de la identidad, pueden conllevar, en muchos casos, la violación de derechos de autor, al utilizar marcas u objetos susceptibles de protección que son de titularidad, por ejemplo, de la entidad propietaria del sistema accedido.

Por último, en el ámbito del Derecho de Patentes, cabe señalar las vulneraciones que de estos derechos se producen a través de los ataques de espionaje industrial que se realizan por medio de Internet (mediante accesos no autorizados, técnicas de sniffing, interceptación de comunicaciones, etc.) como medios de llegar hasta invenciones patentadas o patentables de las empresas.

En definitiva, los elementos tecnológicos están en constante evolución y progresión, lo que permite una mejora constante de redes, servicios, aplicaciones, etc. Un claro ejemplo de esta evolución es el constante aumento de la capacidad para transmitir grandes cantidades de datos a gran velocidad. Sin embargo, esta evolución da lugar a un aumento del riesgo de transmisión de contenidos susceptibles de DPI y un aumento del volumen de contenidos transmitidos contraviniendo la normativa aplicable.

Frente a esta situación de "doble uso" de algunos de los avances tecnológicos en materia de comunicaciones electrónicas, cabe plantear qué papel pueden tener el Protocolo IPv6, en orden a evitar o, al menos, disminuir el número de aquellos comportamientos que, de uno u otro modo, están contraviniendo la normativa sobre Propiedad Intelectual.

Es cierto que el Protocolo no se ha desarrollado con el fin propio de promover la protección de los DPI, pero no es menos cierto que se trata de un desarrollo que procura el cumplimiento pleno de la normativa vigente y que, dado que se viene realizando bajo criterios de optimización, destino a fines, consenso de las partes implicadas en su desarrollo, etc. puede reunir características que por un lado eviten o disminuyan los actos contrarios a la normativa sobre Propiedad Intelectual o por otro lado permitan una mejor respuesta probatoria y judicial frente a los actos de tal tipo que se hubieran producido.

5. La influencia de IPv6 en el ámbito de los Derechos de Propiedad Intelectual

Como es bien conocido, el Proyecto Euro6IX tiene como principal objetivo apoyar la introducción rápida del Protocolo IPv6 en Europa. Con este fin primordial se han definido una serie de resultados finales que, entre otros, van desde el diseño y despliegue de la red hasta el desarrollo de servicios dirigidos a usuarios finales.

El desarrollo del Proyecto Euro6IX incluye la puesta a disposición de redes, servicios avanzados de red, aplicaciones, etc., que podrán ser testeados por los partners del Proyecto,

Derechos de Propiedad Intelectual e industrial

por otros grupos de usuarios o por terceras partes interesadas en intervenir en los resultados del Proyecto, siempre bajo una óptica académica de investigación y avance que, en principio, no tiene como resultado intrínseco la consecución de fines comerciales.

En definitiva, el Proyecto busca realizar desarrollos y pruebas de los elementos intervinientes en cada una de las capas necesarias para la introducción del Protocolo IPv6, lo cual conlleva, lógicamente, el desarrollo de servicios y aplicaciones que, dirigidas normalmente a usuarios finales, van a poder ser utilizados, en algunos casos, para la transmisión de contenidos susceptibles de protección por DPI, por lo que la protección y gestión de tales derechos es un factor que debe ser tenido en cuenta al hacer uso de los servicios y aplicaciones implementados.

En este punto y bajo las premisas señaladas, es interesante hacer una breve reseña de los tipos de direccionamientos de comunicaciones que se definen en IPv6 al objeto de realizar las transmisiones de información y, por extensión, controlar qué y a quién se está transmitiendo. De esta manera, los tipos de direcciones que se pretenden establecer serían:

- Unicast. Este grupo de direcciones se caracteriza por identificar un único punto final de destino (punto a punto). Cualquier contenido enviado a una dirección unicast será entregado a un solo punto de destino.
- Multicast. Las direcciones multicast agrupan un conjunto de puntos finales de destino. Cualquier contenido enviado a una dirección multicast será entregado a un conjunto de destinos que forman parte de un mismo grupo.
- Anycast. Este grupo de direcciones, al igual que el multicast, agrupa un conjunto de puntos finales de destino. La diferencia principal con el multicast está en el sistema de entrega de datagramas. Un datagrama enviado a una dirección anycast es entregado sólo a un punto de destino (el miembro más cercano del grupo al emisor del datagrama)(5).

Bajo estas premisas, se están desarrollando toda una serie de aplicaciones y servicios en cuyo uso va a ser habitual la utilización o transmisión de contenidos, datos, etc. susceptibles de DPI cuya titularidad pueda no corresponder a los intervinientes en la comunicación o transmisión electrónica. En concreto, algunos de los servicios y aplicaciones a través de los cuales se pueden estar utilizando o transmitiendo contenidos susceptibles de DPI son: P2P, videoconferencia, juegos on-line, streaming (audio y vídeo o sólo audio), VoIPv6, Chat/IRC, Messengers, correo electrónico, servicios a la carta o bajo demanda, televisión y vídeo digital, etc.

De tal manera, si bien es evidente que el Protocolo IPv6 no orienta su desarrollo, específicamente, hacia la gestión o protección de DPI, es indudable que el Proyecto Euro6IX es un claro ejemplo de que los desarrollos realizados con relación al propio Protocolo, al definir no

(5) "El protocolo IPv6 y sus extensiones de seguridad IPSec", Verdejo Álvarez, Gabriel. Universitat Autònoma de Barcelona, febrero 2000

sólo la forma de direccionamiento sino también las redes, servicios de red avanzados, aplicaciones, etc., pueden llegar a influir en la forma de proteger tales derechos. En definitiva, de igual manera que en la definición de IPv6 se ha querido tener en cuenta los aspectos legales relacionados con la privacidad y con el posible tratamiento de datos personales, es conveniente resaltar que dentro de los elementos que componen el Protocolo IPv6, existen algunos como, por ejemplo, IPSec, que pueden revestir especial importancia en la configuración de medios tendentes a procurar el control de la gestión y explotación de los DPI aplicables a los contenidos transmitidos, conforme exige la normativa analizada en apartados anteriores de este bloque.

6. La seguridad al servicio de la Propiedad Intelectual

Dada la fuerte competitividad empresarial en todos los sectores y a nivel mundial, la protección de la Propiedad Intelectual, de la información estratégica y de nuevos productos, e incluso la protección de la propia imagen de la empresa, obligan a la adopción de una serie de medidas de control de acceso y de confidencialidad que hacen imprescindible la implantación de sistemas de seguridad suficientemente confiables.

Es por ello, entre otras razones, que la seguridad de la información, entendida en sentido amplio, adquiere un valor fundamental en el desarrollo del Proyecto Euro6IX. Aún más, la seguridad se constituye como un elemento integrador del Proyecto, que se expresa a través del Protocolo IPSec, configurado como requerimiento intrínseco al Protocolo IPv6.

6.1. Aproximación a las cuestiones relativas a seguridad en Internet

En primer lugar, debemos señalar que el concepto de seguridad al que alude el título de este apartado, se define en los términos más amplios posibles, con objeto de cubrir todas aquellas amenazas, físicas y/o lógicas, que afectan a cada uno de los elementos que, en mayor o menor medida, como emisores, receptores o en cualquier condición, intervienen en la Red.

En este punto, es oportuno reseñar el hecho de que, en sus inicios, los Protocolos utilizados en Internet (para establecer la comunicación entre los intervinientes, para el transporte de la información, etc.) no tenían como característica intrínseca el establecimiento de determinados parámetros de seguridad. Es por ello que el avance en el uso de Internet y el crecimiento de su importancia social y económica se ha visto acompañado del aumento paralelo de las vulnerabilidades (entendidas como riesgos que afectan a las comunicaciones, a los sujetos que las realizan o a las contenidos que se transmiten), que buscan aprovechar las zonas débiles que surgen de los fallos de seguridad del tráfico en Internet.

Derechos de Propiedad Intelectual e industrial

Sin entrar en el aspecto técnico de los modos en que se llevan a cabo los ataques o explotaciones de las vulnerabilidades de Internet, sí cabe señalar como ejemplos de amenazas a Internet las siguientes:

- Intrusiones físicas o lógicas sobre los elementos mediante los que se lleva a cabo la comunicación.
- Ataques de virus, gusanos, caballos de Troya, etc.
- Spoofing o enmascaramiento de la identidad de personas, físicas o jurídicas, con objeto de recabar información, acceder a recursos sin la debida autorización, etc.
- Violación de la confidencialidad de las comunicaciones.
- Ataques de Denegación de Servicio, manipulación de información por agentes de intermediación.
- Vulneración de DPI(6).

En definitiva, se viene constatando que la seguridad no fue un requerimiento original de Internet, sino que esta seguridad se viene configurando como un elemento añadido, que da respuesta a la necesidad de herramientas de eliminación o minoración de vulnerabilidades.

6.2. IPSec: el elemento de seguridad del Protocolo IPv6

IPSec es un estándar que tiene como finalidad proporcionar servicios de seguridad a la capa IP y a todos los protocolos superiores basados en IP (por ejemplo, TCP y UDP)(7).

En cuanto a la utilidad que tiene IPSec, principalmente desde el punto de vista del análisis efectuado en este Capítulo, es necesario destacar que IPSec, en resumen, autentifica los equipos involucrados en una transmisión de informaciones, y, en función de la configuración que se establezca, puede llegar a cifrar dicha información para su transmisión entre hosts ubicados en una red (Internet, intranet, extranet, etc.), incluidas las comunicaciones que se establezcan entre un servidor y un terminal, cliente o estación de trabajo y entre servidores. El trabajo de seguridad a nivel de capa IP proporcionado por IPSec tiene como fin principal proveer de protección a los paquetes IP. El Protocolo IPSec está basado es un modelo de seguridad *end-to-end*, de tal modo que únicamente los puntos de la red emisor y receptor deben ser compatibles con el Protocolo y aceptar la protección de la información transmitida.

El Protocolo IPSec viene siendo utilizado (por ejemplo, en la creación de Redes Privadas Virtuales o RPV) con la versión 4 del Protocolo IP (IPv4), pero como adicional o añadido

(6) "IPv6 y la respuesta a la muerte de Alice", Gómez Skarmeta, Antonio F. Departamento de Ingeniería de la Información y las Comunicaciones de la Universidad de Murcia, febrero 2004
(7) "Análisis del protocolo IPSec: el estándar de seguridad en IP"; Pérez Iglesias, Santiago. Revista "Comunicaciones de Telefónica I+D", noviembre 2001

al mismo. Sin embargo, en el caso de IPv6, el Protocolo IPSec se ha establecido como elemento intrínseco u obligatorio en el desarrollo e implementación del mismo, con lo que se provee del mayor grado de optimización a la vertiente de seguridad de la versión 6 del Protocolo.

Asimismo, el Protocolo IPSec, diseñado para funcionar de modo transparente en redes existentes, cuenta, entre una de sus ventajas fundamentales, el haber sido desarrollado sobre el apoyo de estándares del *Internet Engineering Task Force* (IETF)(8), grupo internacional de expertos vinculados a la evolución de la arquitectura de Internet y su óptimo funcionamiento(9). Los resultados de las actividades de los diferentes equipos de expertos se reflejan, entre otras vías, a través de los denominados *Request for Comments* (RFC).

Por otro lado, además de la ventaja de la intervención de IETF en el desarrollo del Protocolo y aún sin entrar en la descripción de su funcionamiento, es posible atribuir al Protocolo IPSec una serie de ventajas propias, que serían, de modo resumido, las siguientes:

- Como ya se ha dicho, se incluye por defecto en el Protocolo IPv6, a diferencia del Protocolo IPv4, donde la integración en el mismo era una mera posibilidad. La obligatoriedad de implementación de IPSec en todos los nodos IPv6, permite que, al establecer una sesión IPv6, siempre sea posible disponer de una conexión segura *end-to-end*.
- Proporciona un nivel de seguridad común y homogéneo para todas las aplicaciones.
- Es independiente de la tecnología física empleada.
- Es compatible con infraestructuras de clave públicas (PKIs).
- Se implementa de forma transparente en la infraestructura de red.
- Es un estándar abierto del sector para proporcionar comunicaciones privadas y seguras. Por tanto, es también un estándar tendente a lograr privacidad, integridad y autenticación. La autenticación y el cifrado de los datos para protegerlos de otros terminales, posibilita la realización de transacciones seguras sobre IPv6. Así, por ejemplo, se podría utilizar el Protocolo IPSec como herramienta que sirviera no sólo para identificar los destinatarios de una transmisión de contenidos amparados por DPI, sino que, además, mediante el cifrado, se estaría evitando la interceptación de los contenidos por terceras partes e, incluso, su posterior reenvío por los destinatarios autorizados a terceros no legitimados.
- Permite asumir el incremento de dispositivos "nómadas", es decir, aquellos dispositivos que reúnen características de movilidad y posibilidad de conexión a diferentes tipos de redes.

(8) "Análisis del protocolo IPSec: el estándar de seguridad en IP"; Pérez Iglesias, Santiago. Revista "Comunicaciones de Telefónica I+D", noviembre 2001
(9) http://www.ietf.org

Derechos de Propiedad Intelectual e industrial

6.3. Descripción del Protocolo IPSec y de sus componentes fundamentales

A través de este apartado se analizan, de forma breve, los aspectos técnicos más relevantes de IPSec, con el fin de facilitar la comprensión de las posibilidades que su adopción conllevaría desde la perspectiva de la protección de los DPI.

IPSec, como primera expresión de su carácter abierto y del esfuerzo de independencia frente a concretos algoritmos de cifrado, es, realmente, un conjunto de estándares para integrar en IP funciones de seguridad basadas en criptografía. Proporciona confidencialidad, integridad y autenticidad de datagramas IP, combinando tecnología de clave pública (RSA), algoritmos de cifrado (DES, 3DES, IDEA, Blowfish), algoritmos de hash (MD5, SHA-1) y certificados digitales X.509 v.3.

La tendencia hacia la neutralidad respecto de los algoritmos utilizados ha llevado a que IPSec se haya diseñado de forma modular, de modo que se pueda seleccionar el conjunto de algoritmos deseados sin afectar a otras partes de la implementación. No obstante, los problemas de interoperabilidad que podían surgir en Internet, han llevado a la definición de ciertos algoritmos estándar que deberán soportar todas las implementaciones que se realicen. De esta manera, los algoritmos de referencia son DES y 3DES, para cifrado, así como MD5 y SHA-1, como funciones de hash. Incluso, es posible usar otros algoritmos que se consideren más seguros o adecuados para un entorno específico.

Dentro de IPSec se distinguen los siguientes componentes fundamentales:

- Dos Protocolos de seguridad: IP *Authentication Header* (AH) e IP *Encapsulating Payload* (ESP), que proporcionan mecanismos de seguridad para proteger tráfico IP.
- Un Protocolo de gestión de claves: *Internet Key Exchange* (IKE), que permite a dos nodos negociar las claves y todos los parámetros necesarios para establecer una conexión AH o ESP.

El Protocolo AH se utiliza con el fin de garantizar la integridad y autenticación de los datagramas IP. Con más detalle, proporciona un medio al receptor de los paquetes IP para autenticar el origen de los datos y para verificar que dichos datos no han sido alterados en su tránsito. No obstante, entre sus características no se encuentra ninguna dirigida a proporcionar confidencialidad sobre los datos transmitidos. En definitiva, el Protocolo AH es una cabecera de autenticación que se inserta entre la cabecera IP estándar (tanto IPv4 como IPv6) y los datos transportados.

El funcionamiento de AH se basa en un algoritmo HMAC (Hashed Message Authentication Code), es decir, un código de autenticación de mensajes. Este algoritmo consiste en aplicar una función hash a la combinación de datos de entrada y una clave, siendo la salida

una pequeña cadena de caracteres denominada "extracto". Dicho extracto tiene la propiedad de ser como una huella personal asociada a los datos y a la persona que lo ha generado, puesto que es la única que conoce la clave.

Por su parte, el Protocolo ESP tiene como fin fundamental proporcionar confidencialidad. A tal fin, especifica el modo de cifrar la información que se desea enviar y cómo este contenido cifrado se incluye en un datagrama IP. En combinación con un mecanismo similar al del Protocolo AH, el Protocolo ESP logra ofrecer los servicios de integridad y autenticación del origen de los datos.

La función de cifrado dentro del Protocolo ESP es desempeñada por un algoritmo de cifrado de clave simétrica. De esta manera, el emisor toma el mensaje original, lo cifra, utilizando una clave determinada, y lo incluye en un paquete IP, a continuación de la cabecera ESP. Durante el tránsito hasta su destino, si el paquete es interceptado por un tercero sólo obtendrá un conjunto de bits ininteligibles. En el destino, el receptor aplicará de nuevo el algoritmo de cifrado con la misma clave, recuperando los datos originales. Como es fácil apreciar, la seguridad de este Protocolo reside en la robustez del algoritmo de cifrado, es decir, que un atacante no puede descifrar los datos sin conocer la clave, así como en que la clave ESP únicamente la conocen el emisor y el receptor.

A los efectos de determinar una utilidad concreta respecto de los procedimientos técnicos analizados en este apartado del Capítulo, se podría tener en cuenta un supuesto hipotético que podría ser, por ejemplo, el caso de una compañía discográfica que pretenda emitir contenidos de su catálogo musical por Internet. A través de estos procedimientos, podría llegar a asegurarse de que dichos contenidos musicales, protegidos por DPI, son recibidos únicamente por los usuarios que, previamente, los hubieran solicitado y hubieran abonado una determinada cantidad de dinero. De este modo, la compañía discográfica conseguiría:

- Confidencialidad del contenido transmitido mediante su cifrado.
- Elección precisa de los destinatarios que van a recibir los contenidos.
- Aportación de garantías, al destinatario, de que los contenidos provienen del emisor correspondiente, que está autorizado para la difusión de los mismos.
- Garantía de integridad de los contenidos protegibles, evitando su modificación por terceros.

No obstante, siguiendo con el ejemplo planteado, independientemente de que la compañía discográfica pueda lograr, al menos, las finalidades señaladas haciendo uso de los protocolos utilizados por IPSec, no es menos cierto que estas ventajas no irían más allá de la concreta transmisión de contenidos a que se refieren, en este caso, la de los archivos musicales. En definitiva, IPSec y, en consecuencia, IPv6 no entrarían en la definición que la normativa

aplicable establece sobre lo que es una medida tecnológica para el efectivo ejercicio o protección de los DPI. Así, no se permitiría restringir el posible reenvío a terceros no autorizados del archivo musical o su transmisión a través de una red P2P.

Sin embargo, pese a no encajar en el concepto de medida tecnológica de protección de DPI, IPSec sí se convertiría en un medio de prueba de gran valor en muchos de los casos de violación de tales medidas realizados en Internet, si se piensa en cada una de las transmisiones telemáticas en que se vulneren esos derechos.

Más aún, el hecho de que IPSec no se configure propiamente como una medida tecnológica tal y como se ha definido no supone que, con el debido planteamiento técnico y jurídico, no pueda llegar a serlo. Planteando esta hipótesis a través de un ejemplo, cabría la posibilidad de incorporar determinada información proporcionada por IPSec a archivos informáticos descargables (por ejemplo música, video, etc.) por Internet con las autorizaciones, licencias, etc. que hubieran determinado los titulares de los derechos aplicables, de tal manera que dicha información sirviera para:

- Determinar qué dispositivos, identificados por su IP, pueden acceder al archivo transmitido.
- Determinar si otros dispositivos, identificados igualmente por su IP, pueden hacer algún uso autorizado (por ejemplo reproducción pero no duplicación) del archivo o si se prohíbe su reenvío a toda persona que no sea su original destinatario.

En definitiva, se trataría de articular los sistemas de gestión de derechos sobre contenidos a través de medidas tecnológicas basadas en IPv6 y, más aún, en IPSec. Esta hipótesis podría ser igualmente operativa en sistemas de Gestión colectiva, que podrían establecer técnicas de control basados en la identificación de usuarios por su IP.

No obstante, como última nota sobre la hipótesis planteada, se ha señalar que su puesta en práctica conllevaría el estudio de cuestiones técnicas y legales que no son objeto de este Capítulo y que podrían matizar o restringir la posibilidad de algunas de las operaciones señaladas.

Volviendo a la descripción de los Protocolos utilizados por IPSec, es evidente que la distribución de claves de forma segura es, por consiguiente, un requisito esencial para el funcionamiento de los Protocolos ESP y AH, como hemos visto anteriormente. Asimismo, es fundamental que el emisor y el receptor estén de acuerdo tanto en el algoritmo de cifrado o de hash como en el resto de parámetros comunes que utilizan.

Esta labor de puesta en contacto y negociación es realizada por un Protocolo de control, denominado IKE, sobre el cual se recogerán sus notas fundamentales más adelante, ya que en este punto del Capítulo cabe hacer una breve referencia a los dos modos de funcionamiento que permite el Protocolo IPSec:

Derechos de Propiedad Intelectual e industrial

- Modo transporte. En este modo, el contenido transportado dentro del datagrama AH o ESP son datos de la capa de transporte. En consecuencia, la cabecera IPSec se inserta inmediatamente a continuación de la cabecera IP y antes de los datos de los niveles superiores que se desean proteger. El modo transporte tiene la ventaja de que asegura la comunicación extremo a extremo, pero requiere que ambos extremos entiendan el Protocolo IPSec.

- Modo túnel. En éste el contenido del datagrama AH o ESP es un datagrama IP completo, incluida la cabecera IP original. Así, se toma un datagrama IP al cual se añade inicialmente una cabecera AH o ESP. Posteriormente, se añade una nueva cabecera IP que es la que se utiliza para encaminar los paquetes a través de la red. El modo túnel se usa normalmente cuando el destino final de los datos no coincide con el dispositivo que realiza las funciones IPSec.

Una vez establecida la cita de los modos de funcionamiento del Protocolo IPSec, se ha de traer a colación un concepto esencial en IPSec cual es el de Asociación de Seguridad (SA, Security Association). Este concepto hace referencia a un canal de comunicación unidireccional que conecta dos nodos, a través del cual fluyen los datagramas protegidos mediante mecanismos criptográficos acordados previamente. Al identificar únicamente un canal unidireccional, una conexión IPSec se compone de dos SAs, una por cada sentido de la comunicación.

Hasta el momento, se ha supuesto que ambos extremos de una SA deben tener conocimiento de las claves, así como del resto de la información que necesitan para enviar y recibir datagramas AH o ESP. Tal como se ha indicado anteriormente, es necesario que ambos nodos estén de acuerdo tanto en los algoritmos criptográficos a emplear como en los parámetros de control. Esta operación puede realizarse mediante una configuración manual, o mediante algún Protocolo de control que se encargue de la negociación automática de los parámetros necesarios, denominándose esta operación como negociación de SAs.

El IETF ha definido el Protocolo IKE (Internet Key Exchange) para realizar tanto esta función de gestión automática de claves como el establecimiento de las SAs correspondientes. Una característica importante de IKE es que es un Protocolo estándar de gestión de claves.

En este sentido, IKE es un Protocolo híbrido que ha resultado de la integración de dos Protocolos complementarios: ISAKMP y Oakley. ISAKMP (Internet Security Association and Key Management Protocol) define de forma genérica el Protocolo de comunicación y la sintaxis de los mensajes que se utilizan en IKE, mientras que Oakley especifica la lógica de cómo se realiza de forma segura el intercambio de una clave entre dos partes que no se conocen previamente.

Derechos de Propiedad Intelectual e industrial

El objetivo principal de IKE consiste en establecer una conexión cifrada y autenticada entre dos entidades, a través de la cual se negocian los parámetros necesarios para establecer una asociación de seguridad IPSec. Dicha negociación se lleva a cabo en dos fases:

1. La fase en la que ambos nodos establecen un canal seguro y autenticado. Dicho canal seguro se consigue mediante el uso de un algoritmo de cifrado simétrico y un algoritmo HMAC. Las claves necesarias se derivan de una clave maestra que se obtiene mediante un algoritmo de intercambio de claves Diffie-Hellman. Este procedimiento no garantiza la identidad de los nodos, para ello es necesario un paso adicional de autenticación.

   Existen varios métodos de autenticación, aunque los dos más usuales son los siguientes:

   - Autenticación basada en el conocimiento de un secreto compartido. Mediante el uso de funciones hash, cada extremo demuestra al otro que conoce el secreto sin revelar su valor.
   - Autenticación basada en la utilización de certificados digitales X.509 v3. El uso de certificados permite distribuir de forma segura la clave pública de cada nodo, de modo que éste puede probar su identidad mediante la posesión de la clave privada y ciertas operaciones de criptografía pública. La utilización de certificados requiere, lógicamente, el previo establecimiento de una Public Key Infrastructure (PKI).

2. En la segunda fase, el canal seguro IKE es usado para negociar los parámetros de seguridad especificados, asociados a un Protocolo determinado, en nuestro caso IPSec.

Durante esta fase, se negocian las características de la conexión ESP o AH y todos los parámetros necesarios. El equipo que ha iniciado la comunicación ofrecerá todas las posibles opciones que tenga configuradas en su política de seguridad y con la prioridad que se hayan configurado. El sistema receptor aceptará la primera que coincida con los parámetros de seguridad que tenga definidos. Asimismo, ambos nodos se informan del tráfico que van a intercambiarse a través de dicha información.

Como último contenido y conclusión del presente apartado, cabe hacer un somero análisis de las características de los servicios de seguridad que ofrece IPSec. Dichos servicios son:

- Integridad y autenticación del origen de los datos. El Protocolo AH parece el más adecuado si no se requiere cifrado.
- Confidencialidad. El servicio de confidencialidad se obtiene mediante la función de cifrado incluida en el Protocolo ESP. Incluso, el Protocolo ESP también tiene herramientas para ocultar el tipo de comunicación que se está realizando.
- Detección de repeticiones. Los Protocolos ESP y AH incorporan un procedimiento para detectar paquetes repetidos. Esta secuencia no podrá ser modificada por el atacante, debido a que se encuentra protegida por medio de la opción de integridad para cual-

quiera de los dos Protocolos (AH y ESP) y cualquier modificación en este número provocaría un error en la comprobación de la integridad del paquete.

- Control de acceso: autenticación y autorización. Dado que el uso de ESP y AH requiere el conocimiento de claves, y dichas claves son distribuidas de modo seguro mediante una sesión IKE en la que ambos nodos se autentican mutuamente, existe la garantía de que sólo los equipos deseados participan en la comunicación. La autenticación válida no implica un acceso total a los recursos, ya que IPSec proporciona también funciones de autorización. Durante la negociación IKE se especifica el flujo de tráfico IP que circulará a través de la conexión IPSec.
- No repudio. El servicio de no repudio es técnicamente posible en IPSec, si se usa IKE con autenticación mediante certificados digitales. En este caso, el procedimiento de autenticación se basa en la firma digital de un mensaje que contiene, entre otros datos, la identidad del participante. Dicha firma, gracias al vínculo entre la clave pública y la identidad que garantiza el certificado digital, es una prueba inequívoca de que se ha establecido una conexión IPSec con un equipo determinado, de modo que éste no podrá negarlo. En la práctica, sin embargo, esta prueba es más compleja, ya que requeriría almacenar los mensajes de negociación IKE y, además, no está definido un procedimiento para referenciar este evento a una fecha concreta.

6.4. PKI

6.4.1. Elementos esenciales de una estructura PKI

Bajo la denominación PKI (Public Key Infrastructure), se agrupan los elementos técnicos y los procesos administrativos necesarios para realizar las operaciones necesarias para, al menos, emitir y revocar certificados de firma electrónica, y, adicionalmente, renovar certificados y cualesquiera otras operaciones añadidas sobre los mismos que se realicen a través de la PKI. Estas operaciones se realizan para una comunidad de suscriptores, entendiendo como tales a los designados en el certificado como titulares del mismo.

La oportunidad de dedicar un apartado a la descripción de la estructura típica de una PKI dentro de este Capítulo no sólo se debe al hecho de que la identificación de los nodos intervinientes en una comunicación en la que se utilice IPSec se puede realizar mediante certificados de firma electrónica, como ya se ha expuesto, sino que la utilización de estos certificados puede tener características, propias o reforzadas, respecto de las que pudieran coincidir con el Protocolo de IPSec, características que podrían utilizarse en la gestión y explotación de DPI.

De esta manera, la creación de PKIs basadas en el Protocolo IPv6, como ya se viene probando dentro del Proyecto Euro6IX, es una posibilidad de gran interés, por cuanto que

Derechos de Propiedad Intelectual e industrial

este tipo de estructuras tiene como fin último crear un sistema confiable basado en la identificación inequívoca de las partes y en la posibilidad de configurar, a medida, el grado de control y confidencialidad de que se quiere dotar a las transmisiones de contenidos realizadas.

En el caso concreto del objeto de este Capítulo, que es la determinación de elementos propios o basados en IPv6 que pudieran ser útiles para procurar el máximo respeto de la normativa sobre Propiedad Intelectual, las ventajas de la utilización de una PKI pueden explicarse a través de un ejemplo práctico: una entidad que quisiera distribuir contenidos protegidos por DPI (películas, música, libros electrónicos, vídeo bajo demanda, etc.) a través de Internet, aprovechando las mejoras de ancho de banda que puede producir IPv6, podría considerar la utilización de un sistema de firma electrónica que, entre otras, reuniera las siguientes funcionalidades:

- Posibilitar la identificación de los receptores de los contenidos, mediante un procedimiento de identificación suficiente y la entrega a los mismos de un certificado electrónico que deberá ser empleado para identificarse antes de hacer uso de los servicios de acceso a los contenidos.
- Permitir garantizar la imposibilidad de acceso a los contenidos por terceros, tanto durante la distribución (por ejemplo mediante cifrado) como posteriormente, ya que se podría establecer que sólo puedan acceder a dichos contenidos quienes dispusieran de un certificado.
- Creación de un canal seguro y controlado de distribución de contenidos audiovisuales vetados para ciertos sectores sociales (por ejemplo menores) ya que se puede articular un sistema reforzado de identificación de los poseedores de certificados que evite que llegue a los miembros de los sectores vetados.

Una vez vistas las características de un sistema de firma electrónica o PKI que podrían ser útiles tanto a los efectos del objeto del presente Capítulo como a los efectos de reforzar las características que pudiera tener, por su parte, IPSec, conviene hacer una breve referencia a los principales elementos que conforman una PKI.

El órgano principal de la PKI, a nivel de responsabilidad sobre las principales operaciones realizadas por la misma, es la Autoridad de Certificación (AC), quien se encarga, al menos, de la gestión y emisión de los certificados. No obstante, también es posible que una misma PKI integre a varias ACs, estructuradas a través de un sistema jerárquico de interdependencia, de tal manera que va a existir una AC raiz, bajo la cual estarán uno o varios escalones jerárquicos, ocupados por el resto de ACs, por lo cual, podrá haber relaciones de dependencia jerárquica también entre los diferentes escalones. La interconexión y dependencia jerárquica entre las CAs se mantiene durante todo el ciclo de vida del certificado, por lo que, por ejemplo, la comprobación del estado del certificado previa a su uso requerirá, asimismo, la comprobación del estado de los certificados de todas aquellas ACs superiores a la AC emisora.

Derechos de Propiedad Intelectual e industrial

La AC también es la encargada de establecer los elementos técnicos y de personal necesarios para el funcionamiento de la PKI. Sin embargo, la AC puede solicitar la ayuda de entidades externas, usualmente otras ACs, para que le provean, en mayor o menor medida, de los elementos técnicos y de personal necesarios para las operaciones de la PKI. Esta decisión no resta importancia al papel de la AC emisora sino que, únicamente, distribuye las operaciones de la PKI. En definitiva, se trata de que la AC, por sí misma o por medios ajenos, establezca una estructura técnica y de personal que provea de confiabilidad a la PKI, tanto desde el punto de vista de operatividad como desde el punto de vista de seguridad de las operaciones.

Usualmente, la compleja estructura administrativa, técnica, de personal, de seguridad, etc., de una AC se viene a reflejar, en sus elementos fundamentales, en la Declaración de Prácticas de Certificación (Certification Practice Statements o CPS), que se establece como soporte documental básico de reflejo del funcionamiento de la AC y del ciclo de vida de los certificados. Por otro lado, los aspectos concretos de la CPS se pueden desarrollar a través de documentos externos o adjuntos a la misma, por ejemplo, los relativos a detalles de seguridad. Una expresión de gran importancia respecto a estos desarrollos complementarios son las Prácticas de Certificación (Certification Practice o CP), en las que se detallan, en su caso, los aspectos propios o particulares de cada tipo de certificado emitido por la AC.

A pesar de la responsabilidad y el control de la AC sobre las operaciones relativas a los certificados, es posible la existencia de la Autoridad de Registro (AR), como órgano encargado, normalmente, de realizar los procesos administrativos relativos a la solicitud de certificados y activar las primeras fases de emisión de los mismos. Las ARs pueden ser órganos propios de la AC o pueden ser terceras entidades independientes.

Por otro lado, descendiendo a los niveles más cotidianos de la vida de los certificados, la primera figura que es necesario resaltar es la del Solicitante, como aquella entidad que manifiesta su voluntad de dotarse con un certificado emitido por la AC en cuestión y que, para ello, inicia los trámites de solicitud establecidos por ésta. Como es lógico, la AC establece una serie de criterios previos que deberán cumplir los solicitantes de certificados, para que éstos, por sí mismos, decidan si entienden que los cumplen o no.

La siguiente figura o elemento a tener en cuenta en una PKI deriva de la figura del Solicitante, ya que éste, una vez comprobados los requisitos necesarios y completado el proceso de solicitud, pasa a adquirir la condición de Suscriptor o Entidad final del certificado. Es decir, pasa a ser, en términos generales, titular del certificado emitido. En esta condición, el Suscriptor del certificado podrá hacer uso del mismo en los términos que se establezcan, al menos, en la CPS y el contrato que haya suscrito con la AC, y asumirá las obligaciones, derivadas de estos documentos, que le correspondan.

Por último, cabe reseñar una última figura, cual sería la del Usuario o Parte confiante, que sería aquella entidad que, como destinatario del certificado y por decisión propia, decide confiar en el mismo. De modo previo a otorgar su confianza al certificado recibido, por cualquier vía, el Usuario, debe haber aceptado al menos, por un lado, el contrato por el que se establecen los términos de uso del certificado y, por otro, la CPS de la AC emisora, a fin de establecer los términos en que se establece la relación de confianza y los roles, obligaciones y responsabilidades de cada parte interviniente (AC, suscriptor y usuario).

6.4.2. Posibilidad de integrar IPSec con una PKI

La posibilidad de utilizar una PKI dentro de las comunicaciones electrónicas que utilicen el Protocolo IPSec, se contempla como una potencial solución a la necesidad de un procedimiento para autenticar de forma fiable a un conjunto de nodos que desean comunicarse mediante IPSec, siendo dicho conjunto de nodos muy numeroso.

Por otra parte, la PKI se articula a través de una organización jerarquizada en la que, normalmente, se centralizan las operaciones sobre los suscriptores de la misma, lo que ciertamente supone una ventaja de esta opción, pues permite dar uniformidad a los criterios de decisión y evita la inseguridad que puede producir la dispersión de los elementos decisorios. En este sentido, no se debe olvidar que, en definitiva, una PKI se basa en factores de confiabilidad, los cuales deben buscarse, en adecuado equilibrio y de manera recíproca, entre todos los intervinientes.

En el caso de IPSec, los sujetos de los certificados, los suscriptores de los mismos, van a ser los propios nodos IPSec. La finalidad o función de los certificados, en este caso, es proporcionar un medio fiable para autenticar la identidad de los dispositivos IPSec. En concreto, cada uno de los dispositivos IPSec dispondrá de un certificado digital que contendrá la clave pública y la información suficiente para identificar de forma unívoca al dispositivo. Esta asociación entre clave pública e identidad está avalada por la firma de la CA integrada en la PKI, que da validez al certificado.

Aunque los Protocolos para la interacción de los dispositivos IPSec con una PKI no están especificados en ninguno de los estándares en que se desarrollan aspectos técnicos relativos a IPSec, sí es muy habitual la utilización, en las PKI actualmente operativas, del estándar X.509 v3 como formato común de los certificados, así como los estándares de la serie PKCS (Public Key Cryptography Standards) para la solicitud y descarga de certificados, lo que puede hacer pensar que van a ser éstos los utilizados para conseguir la referida interacción.

En general, los nodos IPSec necesitan realizar ciertas operaciones básicas con una PKI: acceder al certificado de la AC, solicitar y descargar un certificado, así como comprobar la validez de un certificado recibido. Usualmente, los nodos IPSec realizan la validación de los certificados

mediante consultas de la Lista de Certificados Revocados (LCR) que se almacena en el directorio de la PKI, aunque, caben otras formas de comprobación de la validez de los certificados, como los servicios OCSP (On-line Certificate Status Protocol).

Típicamente, los flujos de comunicación entre una PKI y un nodo IPSec se inician cuando cada uno de los nodos genera un par de clave (pública y privada) y envía una petición de certificado a la AC, en la que incluye información de su identidad y su clave pública. Al mismo tiempo, el nodo descarga el certificado raíz de la AC. A continuación, la AC genera un certificado para el dispositivo IPSec y éste lo recibe. A partir de ese momento, el nodo IPSec podrá usar su certificado en una negociación IKE para autenticarse frente a otros dispositivos. Periódicamente, los dispositivos IPSec accederán al directorio de la PKI para actualizar la LCR.

6.5. IPSec como herramienta de ayuda en la protección de la Propiedad Intelectual

Aunque la función primordial de IPSec no sea la protección o gestión de los DPI que puedan recaer sobre los contenidos, datos, etc. que circulen por Internet o que, en general, se transmitan o soporten en medios electrónicos, parece posible extrapolar ciertos elementos del Protocolo para su utilización con el fin señalado, la protección o gestión de los DPI.

La existencia de direcciones públicas fijas y atribuidas de manera específica a cada punto de la Red, junto con los modos de direccionamiento utilizados por el Protocolo (multicast, unicast y anycast) permiten un primer nivel de control sobre los contenidos transmitidos, ya que se puede determinar, de manera más controlada, los destinatarios y los usos de la información transmitida. Así, por ejemplo, pensando en una transmisión end-to-end de un contenido como, por ejemplo, puede ser una película, dirigido a direcciones unicast o multicast, se podrían obtener, al menos, las siguientes ventajas:

- Se determina con precisión y de manera inequívoca las direcciones IP de destino de la transmisión de contenidos.
- Las características de identificación de IPv6 podrían permitir una sustancial mejora de los métodos de gestión de DPI, independientemente de que la gestión se realice, por ejemplo, por el propio autor o, lo que es más habitual, por una entidad de Gestión Colectiva de derechos. Se podría permitir, de esta manera, una mejor satisfacción de las retribuciones a que tuvieran derecho los titulares de los derechos sobre los contenidos transmitidos.
- Además, la identificación de las direcciones de destino permitiría que, en el caso de contenidos descargables o capturables por medios electrónicos, éstos sólo pudieran ser utilizados por los titulares de las direcciones autorizadas por el emisor, por ejemplo,

sólo por aquellos destinatarios que dispusieran de uno de los números IP que se recojan, como información añadida, en el contenido protegido.

- En los casos en los que se produjera un uso ilegítimo de los contenidos protegidos, los procedimientos técnicos de identificación de los usuarios intervinientes se podrían mejorar en gran medida, ya que, en el caso de Internet, cada usuario, nodo o punto interviniente en el mismo estaría identificado mediante una IP.

Por otra parte y de forma añadida a las posibilidades que se han referido, la utilización de las características de IPv6 para la gestión y explotación de DPI se podría mejorar considerablemente si se utilizan las características de seguridad intrínsecas al mismo, es decir, utilizando IPSec.

En definitiva, las características de IPSec aumentan las posibilidades innatas de IPv6 a la hora de establecer controles más rígidos sobre los flujos de información que se realicen a través de Internet y en los que se incluyan contenidos susceptibles de DPI.

Frente a problemas tan significativos como el intercambio de ficheros con vulneración de DPI a través de redes P2P, o las vulneraciones de marcas o los perjuicios que sobre el rendimiento de la Red y sobre el rendimiento de los medios informáticos de las empresas puede tener el spam, la trazabilidad que posibilita IPv6 y, aún más, con las funcionalidades de IPSec, permitirían llegar a obtener medios de prueba más sólidos ante una hipotética vulneración de la normativa sobre Propiedad Intelectual. Por ejemplo, en el caso de que se detectara una transmisión ficheros de música sin autorización de los titulares de los DPI, podría facilitarse la detección tanto de la fuente de emisión como de aquellos receptores de los ficheros que los están descargando aún sabiendo la ilegitimidad de su actuación.

Aún más, no es descartable que uno de los usos futuros de IPSec sea su posible utilización como técnica o sistema electrónico propio de protección o gestión de DPI, de tal manera que no sólo se securize y optimice la transmisión de información con respeto de los DPI, sino que el nuevo Protocolo pueda servir para que los titulares de los derechos reciban la correspondiente retribución por su explotación. En el caso de las sociedades de Gestión Colectiva de derechos podrían establecer, siguiendo esta posibilidad, sistemas electrónicos de gestión basados en las características de determinación de usuarios a que daría lugar la utilización del Protocolo IPSec.

Por último, cabe plantear otra vía de utilización del Protocolo IPSec para la protección de los DPI, si bien articulada a través de un paso técnico adicional al propio del direccionamiento de las transmisiones o comunicaciones realizadas. Esta vía partiría de la posibilidad de incorporar la información de direccionamiento que establece IPv6 y, en su modalidad segura, IPSec, a los propios datos o archivos transmitidos. De esta manera, el control sobre los destinatarios que permite el nuevo Protocolo se extendería, en su caso, al ciclo de vida de la

información transmitida, pudiendo articularse, posteriormente, mecanismos de control de la utilización "ilegal" de la información, bien por su transmisión a través de medios telemáticos (por ejemplo intercambio en una red P2P), bien por su incorporación a un soporte físico. En este último caso de incorporación a un soporte físico, si se añade la información sobre el transmitente del contenido, se podría comprobar posteriormente si esa fuente tiene las autorizaciones, permisos o licencias necesarios para realizar la acción o si, por ejemplo, ha habido una previa eliminación ilegítima de los medios de protección de los archivos que pudieran haberse establecido por los titulares de los derechos correspondientes.

6.6. IPv6 y la Televisión Digital Terrestre (TDT)

El desarrollo del entorno digital tiene en la Televisión Digital Terrestre (TDT) una de sus expresiones más populares. La TDT se encuadra como una más de las mejoras en el ámbito de las comunicaciones electrónicas que permite una enorme expansión de las capacidades de transmitir contenidos susceptibles de IPRs, al igual que lo hace, de manera propia y significativa, el nuevo protocolo de Internet IPv6.

En consecuencia, cabe plantearse el hecho de que la integración tecnológica entre IPv6 y TDT podría reportar una serie de ventajas, en cuanto a gestión de contenidos susceptibles de IPRs, a igual nivel, al menos, que el que se ha venido señalando anteriormente.

Se debe reiterar el hecho de que el objetivo fundamental del nuevo protocolo IPv6 no es la protección y gestión de los IPRs. No obstante, existirían características del protocolo que podrían llegar a permitir una mejor protección de los contenidos susceptibles de IPRs.

Además, la utilización de IPv6 puede tener consecuencias jurídicas referidas a las partes que intervienen en la emisión de la TDT, incluido el propio usuario o televidente.

Así, cabría plantear la utilización de las técnicas de calidad de servicio (CoS o QoS) en la creación de los paquetes IPv6 utilizados en la prestación de servicios de TDT. Estas técnicas, dado que posibilitan la calificación de la información transmitida a través de los paquetes generados a partir del protocolo IPv6, necesitarían del acuerdo de los operadores TDT (convenios sectoriales, convenios multiparte, acuerdos generados a través de organizaciones internacionales representativas, etc.), en cuanto a la determinación de las reglas de calificación, jerarquías de contenidos, personas autorizadas para realizar la calificación, etc.

Otro supuesto de posible utilización de los recursos que posibilita IPv6 dentro del entorno TDT, podría ser aquel referido al establecimiento de las técnicas necesarias para la restricción de acceso a ciertos contenidos por menores de edad.

Derechos de Propiedad Intelectual e industrial

Por ejemplo, el operador de TDT podría establecer, en el contrato que le una con el televidente, que ciertos contenidos de pago (por ejemplo pornografía) que se soliciten, se vincularán a la dirección IPv6 del receptor del usuario, mediante una emisión basada en el método unicast de IPv6. De tal manera, el operador de TDT podría señalar que, por su parte, se han tomado las medidas necesarias para garantizar que los contenidos pornográficos son accedidos por un usuario concreto y un equipo identificado por su IP, y no por menores de edad que no están autorizados para acceder a dichos contenidos.

Por otro lado, se podrían utilizar las características de IPv6 para gestionar IPRs. En concreto, para proporcionar contenidos audiovisuales a la carta basados el perfil de usuario. Este perfil se encontraría asociado a la dirección IP del receptor de TDT.

De manera simplificada, podríamos plantear un contrato de suscripción a contenidos audiovisuales de pago realizado conforme las siguientes directrices:

- Los contenidos se distribuirán mediante un método multicast a aquellos receptores identificados mediante el Identificador Único de su dirección IP basada en IPv6.
- El pago de los contenidos se realizará mediante una de las siguientes fórmulas:
  - > Contenidos sin publicidad. La bidireccionalidad de comunicación de la TDT permite gestionar el pago sin utilizar un canal diferente (por ejemplo Internet o call-center).
  - > Contenidos con publicidad. El usuario no paga por la visualización de los contenidos, pero acepta la inserción de mensajes publicitarios basados en el perfil de usuario asociado a su IP. El perfil se crea a partir de los servicios integrados en la plataforma TDT que utilice el usuario (canales temáticos, banca electrónica, viajes, hábitos de compra virtual, servicios de ocio, etc.).
- En este ultimo caso, el contrato que regule el acceso a contenidos de pago, habrá de contener las menciones necesarias con relación al tratamiento de datos de carácter personal, principalmente, en cuanto a informar al usuario de los tratamientos de datos personales asociados a su IP basada en el protocolo IPv6 y obtención del consentimiento para dichos tratamientos, a través de la firma (manuscrita o electrónica) del propio contrato.

En definitiva, la integración tecnológica entre IPv6 y TDT permitiría plantear la posibilidad de aprovechar las características inherentes al nuevo protocolo de Internet para configurar adecuadamente ciertas relaciones jurídicas establecidas a partir de la comercialización y utilización de la propia TDT.

Derechos de Propiedad Intelectual e industrial

7. Conclusiones

El objetivo principal de este Capítulo ha sido el estudio de las posibles implicaciones y relaciones que puedan establecerse entre el nuevo Protocolo IPv6 y las normas relativas a la Propiedad Intelectual. Uno de los motivos principales para tomar esta perspectiva surge a partir de la constatación de que las comunicaciones electrónicas e Internet se han convertido en uno de los medios más utilizados para la comisión de actividades vulneradoras de los DPI.

A lo largo del Capítulo se ha reflejado el hecho de que el Protocolo IPv6 no tiene como objetivo propio la protección de DPI ni la generación por sí mismo de fórmulas destinadas a este fin. Esta es la causa de que el análisis que se ha realizado a lo largo del documento con relación al propio Protocolo, a la normativa aplicable, a los problemas actuales de la Propiedad Intelectual en el ámbito electrónico, al protocolo de seguridad (IPSec) integrado dentro de IPv6, etc. se ha enfocado desde el punto de vista de determinar qué características propias del nuevo Protocolo podrían utilizarse en la protección y gestión de DPI.

Es necesario reiterar, no obstante, que no todos los datos o informaciones que vayan a ser transmitidos haciendo uso de IPv6 van a ser susceptibles de protección por la normativa sobre Propiedad Intelectual. Por ello, en el Capítulo se han establecido los aspectos más relevantes que caracterizan a aquellos tipos de datos o contenidos transmisibles y protegibles por los citados derechos.

A partir de estos objetivos iniciales, las principales conclusiones que cabe extraer del Capítulo, con relación a la posibilidad de extender los usos de IPv6 y de su vertiente de seguridad, IPSec, al ámbito de la protección y gestión de los DPI y, en general, al cumplimiento de la normativa sobre Propiedad Intelectual en el ámbito electrónico e Internet, serían las siguientes:

1. El diseño de IPv6 se viene realizando teniendo en cuenta y respetando estrictamente la normativa vigente que le fuera aplicable, tanto en su desarrollo como en su puesta en práctica. Incluso, se ha querido tener en cuenta las implicaciones normativas que pudiera tener el uso de las redes, servicios, aplicaciones, etc. que se vienen desarrollando.
2. Las mejoras en el ámbito de las comunicaciones electrónicas, en constante evolución y progresión avances como el que está destinado a producir IPv6, han mejorado ostensiblemente las capacidades de transmitir contenidos susceptibles de DPI. Pero también, de modo paralelo, han supuesto la creación de nuevas vías, o el aumento de las existentes, para la violación de DPI, cada vez en mayor volumen.
3. La normativa comunitaria sobre Propiedad Intelectual avanza en la creación del marco jurídico de los elementos de protección de los DPI. En esta labor, se vienen estableciendo requisitos normativos en cuya implantación o prueba de su vulneración,

podría ser importante el papel que pueda asumir IPv6 y su vertiente de seguridad IPSec. Así, por ejemplo, las medidas de la normativa comunitaria donde podrían tener una influencia positiva el nuevo protocolo y su vertiente de seguridad son las relativas al reforzamiento de las medidas tecnológicas que los titulares de los DPI pueden establecer para proteger sus legítimos intereses y las destinadas a proteger la denominada "información sobre gestión de derechos".

4. La utilización de IPv6 puede extenderse a la protección de los DPI. Aún teniendo en cuenta que el nuevo Protocolo no se ha desarrollado con objeto de procurar una herramienta de protección y gestión de los citados derechos, es cierto que reúne ciertas características que podrían posibilitar su utilización en ese sentido. Entre las mismas se encuentran las facilidades de identificación de los emisores y receptores de la comunicación electrónica a través de su número IP y las facilidades en la determinación de los destinatarios legítimos de los contenidos protegidos, a través de la tipología de direcciones que se establece dentro del Protocolo (unicast, multicast y anycast).

5. Incluso, la utilización de IPv6 con el fin de procurar una mejor gestión y protección de los DPI podría mejorarse de manera sustancial en caso de configurar la comunicación electrónica con las utilidades de IPSec, protocolo de seguridad integrado de manera necesaria dentro del nuevo protocolo. De manera muy resumida, a los efectos de estas conclusiones, la utilización de IPSec como herramienta de gestión y protección de los DPI daría lugar, al menos, a las siguientes ventajas:

   - Elección precisa de los destinatarios de los contenidos protegidos.
   - Confidencialidad del contenido transmitido mediante su cifrado.
   - Aportación de garantías al destinatario con relación a que los contenidos provengan de un emisor autorizado.
   - Garantía de integridad de los contenidos.

6. En el mismo ámbito, el de la utilización de IPv6 y, dentro del mismo, de IPSec como métodos de protección de los DPI, sería posible plantear la posibilidad de extender esta función hacia la configuración de IPv6 e IPSec, propiamente, como medidas tecnológicas que los autores o titulares de los contenidos protegidos pudieran establecer sobre éstos para restringir su uso por terceros.

7. Se trataría, por ejemplo, de que IPv6 e IPSec no se utilicen sólo para proteger los contenidos durante el direccionamiento y realización de la comunicación electrónica, sino que la utilización como medida tecnológica de protección de derechos podría venir por el hecho de incorporar la información creada por los protocolos a los propios contenidos transmitidos (por ejemplo un archivo musical), de tal manera

que se delimitara el ámbito de usuarios y usos autorizados con relación a unas determinadas IPs y se impidiera, entre otras cosas, la transmisión ilegítima del contenido a terceras partes.

8. En definitiva, la relación entre IPv6 y la protección de DPI no se puede establecer de modo directo, por la ausencia de características en el Protocolo específicamente destinadas a este fin. No obstante, como se ha podido ver a lo largo del Capítulo, dentro de esas mismas características del Protocolo y dentro de IPSec como su vertiente de seguridad, existen algunas de ellas que podrían mejorar de manera importante la gestión y protección de DPI y que, incluso, podrían llegar a convertirse en herramientas técnicas específicas y dedicadas a dichas finalidades y, en general, al cumplimiento de la normativa sobre Propiedad Intelectual.

autores

autores

autores

Consulintel integra servicios y productos de redes y comunicaciones. Empezó su andadura con IPv6 cuando aún no era evidente que este protocolo fuera a ser desplegado en Internet. Hoy Consulintel es reconocida en todo el mundo como una de las empresas líderes y que más ha invertido en I+D+i al respecto de IPv6. Con conocimientos en muy diversos campos relacionados con este protocolo, la empresa ha participado en múltiples proyectos internacionales así como en tareas de estandarización.

Consulintel organiza multitud de eventos de divulgación y formación al respecto de IPv6, entre los cuales se encuentra el Global IPv6 Summit, evento internacional, que en Junio de 2005 ha celebrado su cuarta edición, y al que asisten los más relevantes ponentes de todo el mundo en este campo.

Écija es una firma especializada en servicios jurídicos para empresas, que ofrece asesoramiento multidisciplinar y servicios integrales de calidad. Écija ha sido seleccionada como una de las tres mejores Firmas en España en Nuevas Tecnologías por la prestigiosa guía "The European Legal 500", así como uno de los 30 mayores despachos españoles y el primero en Propiedad Intelectual según el Ranking Expansión 2003.

Écija cuenta con una importante cartera de clientes de referencia en el ámbito de la Sociedad de la Información y, en concreto, asesora a portales de Internet, operadores de telecomunicaciones y desarrolladores de software, así como a destacados organismos públicos y privados.

Écija optimiza sus recursos para proporcionar soluciones a medida, siendo sus áreas de especialización: Mercantil, Procesal, Media & Entretenimiento, Nuevas Tecnologías y Propiedad Intelectual.

El departamento de Ingeniería de la Información y las Comunicaciones de la Universidad de Murcia UMU (España), tiene una experiencia contrastada en áreas como la seguridad de las infraestructuras de red, servicios seguros, seguridad en entornos móviles, control de acceso y desarrollos basados en tarjetas inteligentes. UMU participa en diversos proyectos de investigación nacionales e internacionales, estableciendo colaboraciones con importantes centros e instituciones de investigación como consecuencia de su participación en proyectos del V y VI Programa marco. Adicionalmente el grupo de la UMU tiene colaboraciones con Latinoamérica para la formación de estudiantes de doctorado en diversas áreas como seguridad, servicios móviles y middleware para servicios pervasivos.

En el área de seguridad, el grupo de UMU esta actualmente participando en el proyecto Euro6IX del VPM y en los proyectos SEINIT y POSITIF del VIPM, trabajando en áreas como infraestructuras de PKI, gestión de claves, protocolos de señalización seguros, Sistemas de Gestión de Red basados en Políticas y sistemas de control de acceso basados en nuevos protocolos como PANA.

autores

Basar, Kaisor

Kaisor estudió Derecho en la Universidad de Oxford y amplió sus estudios en el College of Law de Guilford. Solicitor de la Corte Suprema de Inglaterra y Gales desde 1995, trabajó en Lovells y Clyde & Co (una de las 20 mayores firmas de Londres) hasta su traslado a España en 2001. Del 2001 al 2003 fue Responsable del Departamento Internacional de Ecija Abogados, participando en el proyecto Euro6IX.

Carbayo Vázquez, Francisco Javier

Licenciado en Derecho por la Univesidad de Cantabria. Máster en Derecho de las Nuevas Tecnologías en Aliter Escuela de Negocios.

Colabora con los Departamentos de Protección de Datos y Nuevas Tecnologías, así como con la División Tecnológica de la firma, realizando labores de consultoría sobre aspectos jurídicos del desarrollo e implementación de proyectos tecnológicos.

Asimismo, es colaborador habitual en revistas y prensa especializada, habiendo publicado diversos artículos sobre protección de datos, firma electrónica, voto electrónico, facturación electrónica, sociedad de la información y aspectos jurídicos del desarrollo y uso de las tecnologías de la información.

Écija Bernal, Álvaro

Licenciado en Derecho por la Universidad Autónoma de Madrid. Socio de Écija Abogados.

Experto en Derecho Mercantil y Derecho de las Nuevas Tecnologías. Actualmente interviene como Jefe de Proyectos y Consultor Jurídico-Técnico en los Proyectos de Écija relacionados con las Nuevas Tecnologías y la Protección de Datos. Lidera el proyecto de la Unión Europea "Euro6IX" para el estudio del protocolo IPv6 y la protección jurídica de los datos de los usuarios que utilicen dicho protocolo.

Ha intervenido en diversas obras como autor, tales como el *"Libro Blanco del Audiovisual"* e *"Internet: Claves legales para la empresa"*. Asimismo es autor y coordinador de *"Contratos de Internet. Formularios y Comentarios Prácticos"* y *"FactBook de Protección de Datos Personales"*, ambos de la editorial Thomson-Aranzadi. Es ponente habitual en seminarios, cursos y foros de expertos sobre estas materias.

Écija Bernal, Hugo

Socio-Director de Écija Abogados. Doctorando en Derecho Mercantil Internacional. Ha completado estudios de postgrado e investigación en Derecho Internacional, Derecho de la Unión Europea y Propiedad Intelectual en las Universidades de Oslo (Noruega), South Western Community Collage (SWOCC), Coos Bay (Oregón-USA), Seattle (USA). Skidmore Collage (Nueva York, USA)

Su trayectoria nacional e internacional y su dilatada experiencia en diferentes sectores, le han convertido en asesor de empresas líderes, tanto públicas como privadas, así como de proyectos comunitarios e internacionales. Es asesor jurídico de la Comisión Europea en diferentes proyectos de ámbito europeo y, asimismo, es experto en asuntos legales internacionales.

Colaborador habitual en revistas y prensa especializadas nacionales e internacionales como "The John Marshall of Computer and Information Law". Director y Autor de varios libros de gran éxito como el *"Libro Blanco del Audiovisual"*, obra de referencia del sector y el "*Factbook del Entretenimiento 2003"* con la Editorial Thomson Aranzadi.

Fundador y Director del Master de Dirección de Empresas Audiovisuales del Instituto de Empresa. Profesor colaborador en Derecho Mercantil y Propiedad Intelectual en Escuelas de Negocios, como el Instituto de Empresa e ICADE y en Universidades españolas. Es ponente en las mayores empresas de Formación Empresarial en España.

Gil Krokun, Jennifer

Licenciada en Derecho por la Universidad Complutense de Madrid. Máster en Informática y Derecho en la Universidad Complutense. Experta en los problemas de protección de datos en diversas áreas y especialmente en el ámbito de Internet.

Actualmente es Consultora Jefe dentro del Área de Nuevas Tecnologías y Protección de Datos de Écija, liderando Proyectos de Adecuación a la normativa tanto de clientes públicos como privados.

Ha intervenido como autora en la obra *"Factbook de Protección de Datos"* de la editorial Thomson-Aranzadi y es ponente habitual en las mayores empresas de formación empresarial y Universidades españolas.

Gómez-Skarmeta, Antonio F.

Antonio F. Gómez Skarmeta recibió el título de Ingeniero en Informática por la Universidad de Granada y de Doctor en Informática por la Universidad de Murcia (España). Desde 1993 es Profesor Titular de Universidad en el departamento de Ingeniería de la Información y las Comunicaciones de la Universidad de Murcia, y desde 2001 director del mismo. Ha estado

trabajando en varios proyectos de investigación, principalmente de ámbito nacional, en el campo de la inteligencia artificial (proyecto M2D2), tele-enseñanza, trabajo colaborativo o nuevos servicios telemáticos para redes de área extensa (SABA), además de diversos proyectos europeos en las áreas de entornos colaborativos, seguridad en redes IP así como movilidad y seguridad en IPv6, desarrollando servicios avanzados relacionados con IPv6 como multicast, seguridad etc. Ha publicado más de 130 artículos en congresos, y revistas nacionales e internacionales, siendo además miembro de diversos comités de programas.

Martínez, Gregorio

Gregorio Martínez es Ingeniero en Informática y Doctor en Informática por la Universidad de Murcia. En 1997 comenzó su labor profesional en el Servicio de Informática de dicha Universidad participando en varios proyectos relacionados con la seguridad en las comunicaciones. En 1999 comenzó como personal investigador en el Departamento de Ingeniería de la Información y las Comunicaciones de la Universidad de Murcia, gracias a una beca FPU del Ministerio de Educación y Ciencia. En el 2001, accedió a una plaza de profesor en el mismo Departamento.

Su labor científica e investigadora se ha centrado principalmente en los aspectos de seguridad y gestión distribuida de las redes de comunicaciones IP (tanto IPv4 como IPv6). En la actualidad se encuentra colaborando en varios proyectos de investigación nacionales e internacionales relacionados con estos temas como, por ejemplo, los proyectos europeos Euro6IX, SEINIT o POSITIF. También mencionar que ha publicado varios artículos en conferencias y revistas tanto nacionales como internacionales.

Palet Martínez, Jordi

Jordi Palet Martínez, CEO/CTO de Consulintel, ha trabajado en informática, redes y telecomunicaciones desde hace más de 20 años.

Ha estado involucrado en el IPv6 Forum, como presidente del grupo de trabajo de Educación y Promoción, desde la fundación del mismo y es miembro del Directorado Técnico. Jordi es también miembro del IPv6 Logo Committee, responsable del Programa "IPv6 Ready".

Jordi frecuentemente imparte conferencias en eventos en todo el mundo, al respecto de IPv6 y aspectos relacionados (Calidad de Servicio, multidifusión, anycast, mobilidad, seguridad, multihoming, ...) y su involucración en proyectos de Investigación y Desarrollo.

Participa activamente en organización de estandarización y similares como ISOC, IETF, RIPE. Trabaja también en el IPv6 Task Force de la Comisión Europea, donde ha sido unos de los principales contribuyentes Es co-autor de numerosos documentos en IETF.

Jordi es miembro activo de organización sin ánimo de lucro para la divulgación de tecnologías de comunicaciones e Internet. Igualmente participa en el IPv6 Task Force Español, el IPv6 Task Force Steering Committee. Coopera con diversas organizaciones Europeas y de todo el mundo como los IPv6 Task Forces y organizaciones similares.

Jordi participa en diversos proyectos de I+D y fue el diseñador de Euro6IX, así como el coordinador científico del proyecto. Está implicado también en otros proyectos IST, como 6POWER (donde también es el coordinador científico), 6QM, Eurov6, IPv6 TF-SC, 6LINK y el IPv6 Cluster. Igualmente esta involucrado en otros proyectos I+D nacionales y el proyecto Eureka PlaNetS.

Sáiz Peña, Carlos Alberto

Licenciado en Derecho por la Universidad de Alcalá. Máster de Práctica Jurídica de la Universidad Pontificia de Comillas (ICADE). Estudios Superiores en materia de Propiedad Intelectual y Derecho de las Nuevas Tecnologías. Socio de Écija Abogados.

Actualmente lidera el Área de Nuevas Tecnologías y Protección de Datos de Écija, dirigiendo los Proyectos de Consultoría y Adecuación a la normativa de protección de datos de grandes empresas y multinacionales clientes de Écija. Asimismo desarrolla una importante labor en el impulso de todas las iniciativas de la firma relacionadas con las Nuevas Tecnologías a nivel asociativo, institucional y formativo.

Ha intervenido en diversas obras como autor, tales como el *"Libro Blanco del Audiovisual"* e *"Internet: Claves legales para la empresa"*. Asimismo es autor y coordinador de "*Contratos de Internet. Formularios y Comentarios Prácticos"* y *"FactBook de Protección de Datos Personales"*, ambos de la editorial Thomson-Aranzadi. Es ponente habitual en seminarios, cursos y foros de expertos sobre estas materias.

figuras y enlaces

Tabla de figuras

Enlaces a IPv6

- Euro6IX http://www.euro6ix.org
- IETF http://www.ietf.org
- IPv6 Task Force http://www.ipv6tf.org


Euro6IX
IPv6:The New Internet


European Commission


Information Society
Technologies


Consul inTel
Consultores Integrales en Telecomunicaciones


ECIJA