socialize
service oriented assisted living infrastructure

WP 1 – Definition of Scenarios and Requirements – Assessment of Socio Economical and Technological Impact

Document: D1.4 Security and Privacy guidelines document

Date: 30/03/2016

Confidentiality: ☑ Public ☐ Restricted

Version: ☐ Draft ☑ Final

AAL PROGRAMME

DOCUMENT INFORMATION

Acronym of lead partner for the deliverable	IRIS
Work package	WP 1 - Definition of Scenarios and Requirements – Assessment of Socio Economical and Technological Impact
Contractual date of delivery	March 2016
Date of delivery	April 2016
Nature	Report
Dissemination level	Public

Document Responsible	IRIS (IT)
Author(s)	IRIS (IT)
	ISTI–CNR (IT) [Dario Russo, Vittorio Miori, Loredana Pillitteri]

Release	1
Version	3
Date	10 04 2016

REVISION HISTORY

Date	Version	Author	Paragraph added/modified	Description
20/12/2015	1	ISTI-CNR		First draft Section 3 Privacy
29/03/2016	1	ISTI-CNR		First draft Section 3 Privacy
29/03/2016	2	IRIS		Document Revision Section 1,2 Security
02/04/2016	2	IRIS	2.2, 2.3	Section 2 Security
10/04/2016	3	IRIS		Document Revision Section 2 Security

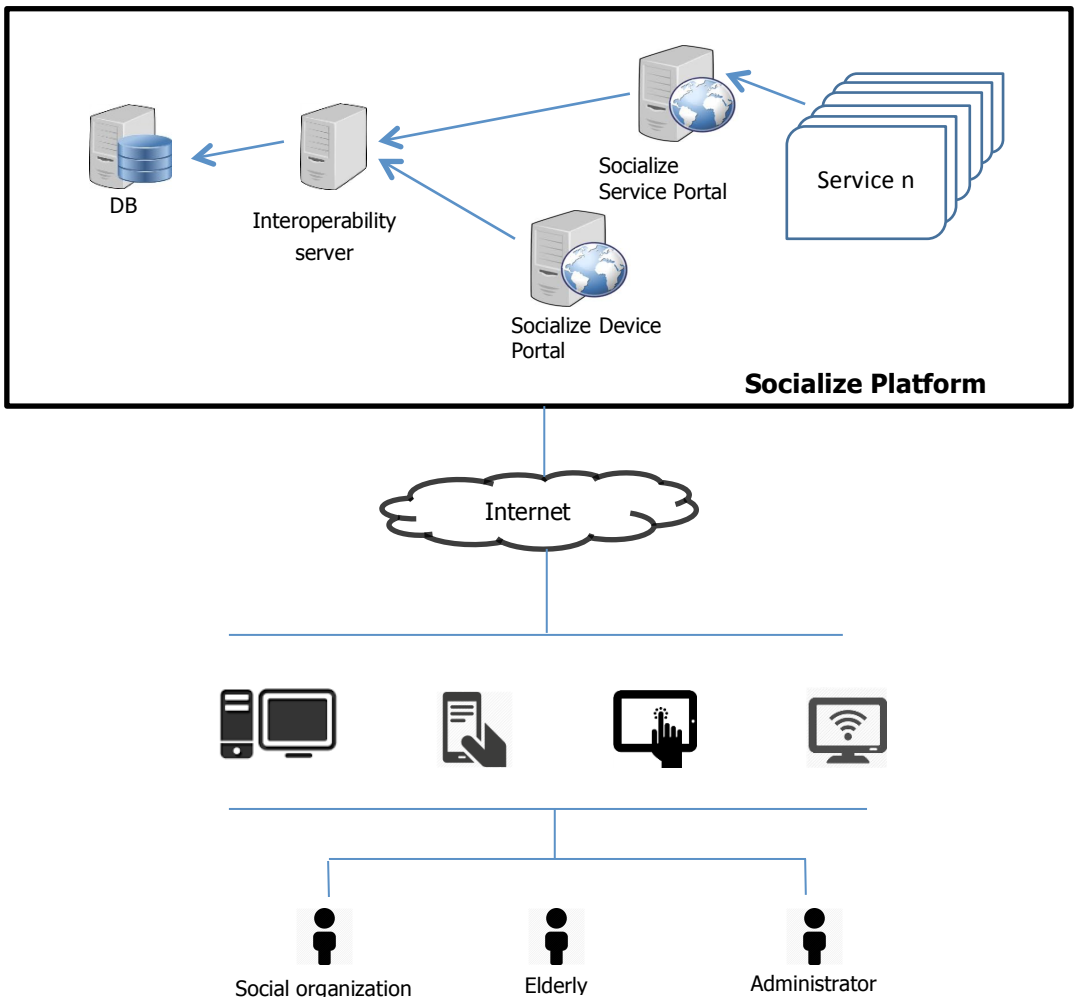
TABLE OF CONTENTS

1. INTRODUCTION

1.1. PURPOSE

The purpose of this document is to provide guidelines to build a system that is secure and assure data integrity and privacy.

1.2. ENVIRONMENT OVERVIEW



2. SECURITY

2.1. INTRODUCTION

Application security is the use of software, hardware, and procedural methods to protect applications from external threats.

As you analyse your infrastructure and applications, you identify potential threats and understand that each threat presents a degree of risk. Security is about risk management and implementing effective countermeasures.

Security must be applied at three layers: network, host and application

2.2. SECURING NETWORK

SOCIALIZE is a service oriented platform that could be potentially accessed from anywhere in the world. However, the access to services should be granted to authorised endpoints. Any organisation wishing to connect to SOCIALIZE, independently from its role that could be service user or service provider, is responsible for ensuring that their SOCIALIZE connection does not compromise the security measures already in place within the WAN (Wide Area Network).

All Socialize service Applications should provide encryption for data using Transport Layer Security (TLS)2 or an equivalent security standard. It is therefore advisable that the appropriate measures are taken with existing systems to ensure that sensitive data is secure before connecting to SOCIALIZE.

Administrators can configure Internet Protocol Security (IPSec) enforcement, IEEE 802.1X enforcement, virtual private network (VPN) enforcement, Dynamic Host Configuration Protocol (DHCP) enforcement, or all four, depending on their network needs.

2.2.1. NETWORK ADMISSION CONTROL

A Network Admission Control (NAC) solution compares the security state of a device, which is attempting to connect to a network, to a set of policy attributes that define what security conditions must be met to allow network access. The scope of a NAC solution must encompass external and internal network connections by managed and unmanaged devices.

Examples of unmanaged devices include ‘rogue’ systems and servers that are deployed outside central Information Technology (IT) management control, in addition to contractor PCs and employees' home machines. The NAC solution should cover the following network connection scenarios:

- VPN —IPsec and Secure Sockets Layer (SSL)
- LAN — wired and wireless connectivity

2.2.2. SECURITY

A layered approach to security is recommended. This approach provides a defence in depth posture, which reduces the scope of any security breaches. The recommendations will also assist organisations in meeting the European and National requirements for the protection of Person Identifiable Data (PID) whilst in transit, and the requirements of the Confidentiality SOCIALIZE Code of Practice.

This model uses a layered architecture of distinct modules or building blocks, with each layer responsible for a specific role in the support of the end-to-end delivery of information. The benefits of a layered architecture are: -

- Scalability.
- Ease of implementation.
- Ease of troubleshooting.
- Predictability.
- Manageability.

Each of the layers supports distinct functionality or requirements. Layers can be added to the model to support additional functionality. As an example, an Internet or public access layer can be added to complement an existing layered infrastructure.

The hierarchical network design model is comprised of four basic layers:

2.2.2.1. CORE LAYER

This provides high-speed IP connectivity between the distribution, access and server layer LAN switches via two or more high availability core switches.

2.2.2.2. DISTRIBUTION LAYER

This layer is where elements such as security and QoS policies are enforced to control how the network will service individual information flows. This layer can be a physically separate layer of switches, or a logical layer located within the core switches. This will be dependent on the size of an organisation's network infrastructure.

2.2.2.3. ACCESS LAYER

This layer provides connectivity for systems such as end user workstations and printers. The access layer enforces admission and control policies, and provides the logical segmentation of devices into groups – Virtual LANs (VLANs) – which share common functional requirements. The access layer also provides a 'trust' boundary where

application traffic can be identified and classified for appropriate servicing by the distribution and core layers.

2.2.2.4. SERVER LAYER

This layer provides high-performance connectivity and resilience, and secures access to the application servers. The server module is distinct from an access layer module because of the differing requirements between user and server connectivity. For example, availability is much more of an issue within the server module than typically within access modules supporting general network users.

2.2.2.5. ACCESS LAYER RACCOMANDATIONS

- Physical locations and wiring closets for active equipment deployment should be physically secured against unauthorised access.
- The network devices should support 10/100Mb switched Ethernet connectivity, with 10/100/1000Mb switched Ethernet being desirable.
- Equipment level redundancy and redundant / backup power should be provided to access layer devices that are supporting critical clinical areas and users.
- The network devices should support the provisioning of 802.3af Power over Ethernet (PoE).9
- The access layer should use at least two resiliently configured fibre or copper uplink trunk connections to two separate distribution / core layer locations.
- The access layer should provide the 'organisational boundary' for the classification / marking of application traffic for subsequent prioritisation and scheduling across the organisation's network infrastructure.
- The network devices should support intelligent security services and features to help maintain the confidentiality of PID whilst in transit.
- The network devices should support intelligent security services and features to help mitigate unauthorised connections to the network infrastructure.
- The access layer should include comprehensive management tools for device, fault and performance management. In particular the tools should support network-wide software and configuration updates, and network-wide deployment of QoS and security policies.
- The network devices should support secure management protocols such as Hypertext Transfer Protocol Secure (HTTPS), Simple Network Management Protocol Version 3 (SNMPv3), Secure File Transfer Protocol (SFTP) and Secure Shell (SSH).

2.2.2.6. CORE AND DISTRIBUTION LAYER RECOMMENDATIONS

- The Core and Distribution layers should support Ethernet connectivity at speeds up to 1Gbps, with 10Gbps being desirable.

- Distribution and Core inter-switch links should be a minimum speed of 1Gbps.
- Core / Distribution Layer inter-switch links (trunks) should be logically bundled for additional resilience and performance. It is preferable to utilise bundling and channelling technologies that are transparent to the link and network layer protocols.
- Links or trunks between core and distribution switches should be controlled by a layer 3 routing protocol.
- The Layer 3 protocol controlling network convergence should be tailored to minimise failover times, and hence minimise application interruption.
- The Distribution layer should provide the capability to enforce the organisational QoS policy through intelligent queuing, scheduling and congestion avoidance mechanisms.
- The Distribution layer should support intelligent security services and features to help maintain the confidentiality of PID whilst in transit.
- The Distribution layer should support intelligent security services and features to help mitigate against unauthorised connections to the Network Infrastructure.
- The Core and Distribution layers should provide comprehensive management tools for device, fault and performance management. Specifically the tools should support network-wide software and configuration updates, and network-wide deployment of Quality of Service and security policies.
- The Core and distribution layer should support secure management protocols such as HTTPS, SNMPv3, SFTP and SSHv2.

2.2.2.7. SERVER LAYER RECOMMENDATIONS

The availability of Server resources is often critical to large organisations, and the design of the server layer should therefore reflect the higher level of resilience and performance that is required.

It is recommended that:

- The Server layer should support 1Gbps Ethernet connectivity. It is desirable that the infrastructure offers support for 10Gbps Ethernet where possible.
- The infrastructure should utilise equipment level redundancy, and offer redundant or backup power services.
- Support should be provided for dual attaching servers. Note this may not be possible with some operating systems and some applications, therefore dialogue with server and application suppliers is essential.
- The server layer should utilise dual uplink connections to the Core layer.
- The server layer should provide the organisational boundary for application traffic, and should support the capability to classify and mark application traffic for subsequent prioritisation.

- Intelligent security services and features should be provided to help maintain the confidentiality of PID whilst in transit.
- Intelligent security services and features should be utilised to help mitigate against unauthorised connections to the Network Infrastructure.
- Comprehensive management tools for device, fault and performance management should support the server layer. In particular the tools should support network-wide software and configuration updates, and network-wide updates for QoS and security policies.
- The Server layer should support secure management protocols such as HTTPS, SNMPv3, SFTP and SSHv2.

2.2.3. NETWORK INFRASTRUCTURE AVAILABILITY

High availability can be achieved by the use of a well-designed network infrastructure to support the enforcement of a strong security policy, and the implementation of resilience and redundancy features within the network infrastructure components. The resilience features can be grouped into two basic categories – Physical resilience and Software resilience.

The supporting infrastructure, cable plant, physical environment and active component all fall into the physical category. Network control plane features, such as layer two and layer three routing protocols, DHCP, and Domain Name System (DNS) services fall into the software category.

2.2.4. PHYSICAL RESILIENCE AND REDUNDANCY

It is essential that fundamental knowledge of the physical layout of the network is known and documented. Node points for the Core and Distribution elements of the network should be identified, in addition to wiring closet locations for distribution to network endpoints. Distances between network locations should be determined before laying cables - both for fibre-optic cabling and structured copper wiring. The measured distance for fibre optic cabling may dictate the mode of cable used, whilst structured copper wiring has a fixed maximum distance.

It is recommended that multi-core single mode fibre-optic cable is used between core layer switch sites, and between uplinks from wiring closets to distribution layer / core layer switches, as a minimum standard.

- It is recommended that fibre-optic cable connecting Core layer infrastructure components should be laid within diverse routing paths. Such connections may be bundled together to create aggregated links.
- It is recommended that cables are laid from wiring closets to a minimum of two distribution / core layer switch locations.

2.2.5. EQUIPMENT LEVEL REDUNDANCY

The provision of redundant or load sharing equipment in a network is a trade off between budget constraints and pragmatism over the likelihood of an outage. The financial impact of such measures has often dictated that specific areas of the network are prioritised for redundancy. However as the IP network becomes the single vehicle for delivery of local and national healthcare applications, greater emphasis should be placed upon providing heightened levels of redundancy across the whole of the network infrastructure.

It is recommended that the organisation's network infrastructure should have two or more core switch node locations. Each wiring closet / Distribution layer switch should have at least two uplinks to separate Core / Distribution layer switches.

- Core switches should be deployed with redundant management engines, switching fabrics and power supplies. Where there is a heightened level of dependency on one core switch, e.g. where cable plant restrictions result in distribution / wiring closet uplinks being terminated by a single core switch, the distribution of the uplinks across separate line cards within the core switch should be considered essential.
- It is recommended that where a single chassis is utilised in the wiring closets, the uplinks are distributed across line cards within the chassis in order to decrease the risk of an outage in the event of a failure of any one card in the chassis.
- It is recommended that where stackable switches are used in the wiring closets, these should be stacked together to create a single logical access layer switch. This should be achieved either through the uplink ports or optimally via dedicated bus connections if available. The uplinks from the switch stack to core / distribution node locations should be via separate switches in the stack wherever possible.
- Where stackable switches are used, the insertion and removal of switches in the stack without disruption to network traffic is desirable.

2.2.5.1. SOFTWARE RESILIENCE AND REDUNDANCY

Software features within the infrastructure devices to converge around physical failures perform a vital role in ensuring an application's availability. For example, the capability to create one logical link from two or more physical links, and "hide" individual link failures from higher layer networking protocols, enables the infrastructure to re-route traffic around link failures transparently to the end user / application.

The use of layer three routing protocols enables a more scalable approach to alternative path switching around failures. When considering the choice of Layer 3 routing protocol, flexibility, convergence capabilities, and scalability should be considered.

Link state protocols, such as Open Shortest Path First (OSPF)11 and Intermediate System-to-Intermediate System (IS-IS),12 are the preferred options. OSPF is found to be the most common protocol in use and has the added advantage of being an accepted industry standard suitable for multi-vendor networks.

Both OSPF and IS-IS offer enhanced security features. Passwords can be set to prevent unauthorized routers from forming adjacencies with routers in the network, and MD5 Authentication is an option.

Some vendors support proprietary layer 3 routing protocols such as Cisco's Enhanced Interior Gateway Routing Protocol (EIGRP),13 which are often less complex and are able to provide faster convergence times. These protocols should only be considered for single vendor networks or if the vendor also provides layer 3 routing protocol intercommunication capabilities. This is usually achieved through route re-distribution between the layer three routing protocols. The transfer of routing information between routing processes should be treated as an autonomous boundary point in terms of security posture. For example, route re-distribution should be secured against unauthorised route injection and spoofing.

At the layer 3 / layer 2 boundaries, a first-hop routing protocol should be used to provide a virtual default gateway. The standards based first-hop routing protocol is Virtual Router Redundancy Protocol (VRRP).14 Vendors who provide proprietary first-hop routing protocols can provide enhancements such as awareness of upstream network events and active / active uplinks concurrently. Vendor proprietary solutions should only be considered where the first hop routing protocol is intended to be utilised between devices from a single vendor that are performing the virtual default gateway function.

Whilst Layer 3 is recommended for the network core, it may be necessary for Layer 2 traffic to traverse the network to support legacy non-routable protocols. Whilst some vendors have introduced their own proprietary enhancements to the Spanning Tree Protocol (STP),15 there are two standards based enhancements to STP available: -

- The IEEE 802.1s standard allows several VLANs to be mapped to a reduced number of spanning-tree instances.
- The IEEE 802.1w standard provides the mechanisms to allow faster spanning tree convergence after a topology change.

2.2.5.2. SECURITY POLICY MANAGEMENT

The security posture of a network has a significant impact on the availability of that network infrastructure. A malicious worm or virus outbreak has the potential to consume all available resources, starving legitimate clinical applications of bandwidth and processing power. The effect to the end user is a lack of availability.

Policy management tools are required to create and implement an organisational security policy in a consistent manner. The tools should additionally be capable of proactive monitoring, the correlation of generated events and the ability to generate

notifications and intelligent responses to those events. For example, the appropriate action for intrusion attempts that are stopped at the perimeter is generally to simply log the event, whereas intrusion attempts that are arriving on servers require further investigation. The number of events generated can be significant, to the extent of becoming impractical for events to be processed by human analysis alone. Policy management tools should therefore support automated processes for the filtering and prioritising of events.

Network infrastructure devices should be capable of actively participating in the security policy in terms of access authorisation, legitimate usage, audit and accounting.

- All security events should be logged and assessed against the security policy for appropriate action.
- The use of active monitoring and auto-processing of events is highly recommended, especially where behavioural based anti-virus software for end user workstations is deployed.
- It is recommended that organisations deploy network based Intrusion Detection Systems (IDSs) and Intrusion Prevention Systems (IPSs), and utilise behavioural based anti-virus technologies on end systems
- It is recommended that organisations deploy centralised anti-virus and patch management systems to enable better management, control and reporting.
- It is recommended that security management tools are used to manage all security devices and processes within the network. It is desirable that event correlation and analysis from multiple sources is supported by the security management platform.

2.2.5.3. WIDE AREA NETWORK LINK CONSIDERATIONS

Where SOCIALIZE partner organisations have a responsibility to facilitate connections to other sites, either within their organisation or as connections to 3rd Parties.

An additional consideration is about back-up circuits. These could be either lower speed back up lines or identical access links that are load balanced. If a lower speed backup service is chosen, the effect on applications during the back-up period should be carefully considered.

- It is recommended that back-up circuits and equipment should be provided for WAN links that carry critical application data.
- QoS policies and controls can be critical in WAN environments where the change is made from high speed LAN connectivity to comparatively low WAN bandwidth. This can dictate a need for prioritisation of latency sensitive traffic and for mechanisms such as rate limiting and fair sharing techniques.
- It is recommended that an organisation's QoS schema accounts for WAN link failure scenarios, and ensures that sufficient resources are allocated to critical applications across WAN back-up links.

- All WAN links which are not wholly and exclusively within the control of the organisation should be viewed as being insecure, and therefore would require appropriate measures to ensure confidentiality is maintained for PID whilst in transit.
- Where 3rd Party connections are established, strict control of access must be in place that is in accordance with National and European security policies.

2.2.6. FIREWALL GUIDELINES

Firewall Technologies have typically been the most common way to secure user and/or system access from a higher security level environment to a lower security level environment in a secure and efficient manner. The firewall can also grant access from lower security to higher security level environments but at a more granular level.

With the boundaries between networks now becoming more blurred, and high speed links frequently available, the choice of what firewall technology solution(s) to implement is increasingly more difficult. In addition to the roles a firewall has traditionally performed new functions and services are also becoming increasingly available which adds value to the device and gives a better Return on Investment (ROI).

Network Designers now have to think not only for today's need but also for likelihood of network growth and other influencing factors, while still maintaining a highly available and secure network, often at the heart of which are firewall technologies.

2.2.6.1. CLASS OF FIREWALLS

There are four main classes of firewall, which can be implemented on both the hardware and software options mentioned in the last section. These are detailed in this section and comprise:

- Packet Filter Firewalls
- Stateful Inspection Firewalls
- Application Proxy Firewalls
- Deep Packet Inspection Firewalls

The class of the firewall largely determines its capabilities and therefore its ability to protect an organisation's network. Some classes are better suited to specific environments, whilst other classes may be used with a mixture of environments in order to provide a more robust solution.

All firewall classes have common characteristics in that they use certain criteria in order to identify good traffic which is permitted and bad traffic which is not permitted. This will be determined according to the security and access policy in place. When traffic traverses a network it does so in a packet at the network layer. This packet holds information pertaining to the connection taking place, which includes but is not limited to:

- Senders source address

- Recipients destination address
- Service to which the packet pertains (usually port number)
- Network operation and status flags
- Actual payload of data to be delivered

2.2.6.1. DESIGN CONSIDERATIONS

When planning a firewall deployment it is critical to assess certain criteria to choose a product offering that will suit the organisations needs within budget. Some of the key areas are discussed in this section.

Firstly it is beneficial to identify what is being secured, the higher level of security required, the more robust the security solution deployed.

There are various standards authorities that firewall vendors can submit their products to in order to have their security claims tested and verified (i.e. ICSA Lab Certification (USA), CESG (UK)) .

Once the networks to be secured have been identified, a strategy must be defined to determine how to accomplish this. There may be several elements from the firewall goals section to include and it is important to choose a device that will adequately support these requirements. Vendor websites will often detail a product's capabilities, though it may be possible to obtain software or hardware on evaluation before committing to a particular product for your solution.

2.2.7. PERSONAL AREA NETWORK

A Personal Area Network (PAN) comprises a set of wireless medical sensors associated to a user that are used to sense his vital signs. PANs are not isolated but may interact, coexist, and become a part of a world of professional Medical Sensor Networks (MSNs), each comprising several thousands of sensors, accommodating other users's PANs, and being operated by very diverse organizations, such as surgeries, fitness centers, hospitals, or retirement homes. Ubiquitous MSNs and PANs allow for pervasive health monitoring in a multitude of environments and locations and are one of the main enablers of pervasive healthcare as they allow sensing and accessing medical data of users on the fly, independently of location, time, or users involved. In such a pervasive health system, only authorized parties, such as medical staff, family, or sport trainers are permitted to access to sensed health information of users. The exchange of users' medical data leads to privacy and security issues, hence basic security services are required. These concerns become especially important when many users and health institutions need to interact with each other.

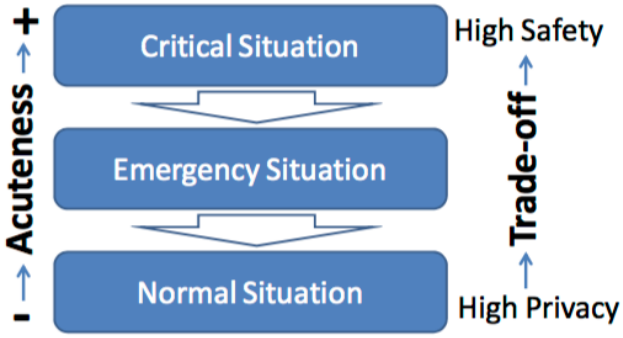
Efficient and reliable access control is a key requirement in this setting in order to ensure that only authorized staff has access to private medical data. This is requested by users, and also legally enforced by European Directive 95/46.

2.2.7.1. APPLICATION AND TECHNICAL NEEDS

Allowing for rapid and accurate response to events or access requests of variable acuteness in medical sensor networks is a must. Along with that there is a need of an access control system for sensor networks in which the access control decisions and the delay response depend upon the health acuteness of the user.

For instance, an authorized doctor might have to wait a few seconds for the medical data of a healthy patient while a sensor node verifies his access control roles or a nurse might not be able to access some data in a normal situation. However, in an acute situation in which the user's life is in danger, the doctor should receive the information immediately and the nurse should have access to the user's information.

The above requirement is represented in Figure 1 as a trade-off between safety, privacy, and access control in different contextual situations. This is especially important in medical sensor networks as the medical staff can directly interact with the PANs' sensors. Such a setting is completely different from traditional centrally systems in which a single backend intelligence takes the access control decisions. Here, the sensors comprising the PAN of a user should be able to decide in a dynamic way on the disclosure of the sensed data.



2.3. SECURING HOST

2.3.1. SYSTEM HARDENING

The term 'system hardening' refers to taking a typical or default installation of an Operating System (OS), associated applications or network device and then modifying the configuration to decrease the systems potential exposure to threats. The extent of hardening depends on the role the system performs and can include the following:

1. Turning on security controls (i.e.BIOSpasswords,safe_modeinPHP)
2. Removing unnecessary services, applications and network protocols
3. Removing default accounts and changing default passwords
4. Installing security solutions (i.e.AntiVirus, Encryption)

5. Installing security patches and updates
6. Implementing strict ACL's (permissions)

It is the recommendation of the Socialize Technical Team that sufficient policy is in place that stipulates that no system should be deployed prior to being hardened. The policy should also contain the following:

- The purpose and scope of the policy
- Stipulation of periodic assessment
- Appropriate and enforceable sanctions
- Review date or criteria based on update triggers i.e. technology change,
- regulatory compliance requirements
- Links to hardening standards that have been approved

This policy should be signed off at the highest level (i.e. CISO, CIO, CEO) by each SOCIALIZE Project partner involved in system development and deployment to ensure that the policy has the appropriate authority.

It is also recommended that the system hardening process be built into all SOCIALIZE partners change control processes. This will provide a means of ensuring that the hardening process is completed and signed off at all relevant levels within the project.

The hardening process should be based on a combination of 'risk assessment' and 'business requirements'. For example, if there is a business requirement to have a particular security control turned off then this should be subject to a risk assessment.

2.3.1.1. HARDENING BASICS

There are a number of basic hardening steps that all SOCIALIZE partners should and can do. Although not comprehensive in nature they provide a quick and easy way of mitigating some of the more common methods attackers utilise to compromise system security. These are:

- Change all default passwords and remove/disable all unused user accounts (remember that some systems come with a multitude of default username and passwords and not just an "administrator" account)
- Remove all unnecessary software and services
- Turn on built in security measures i.e. built in firewall, enable bios passwords
- Install Anti Virus (if system requires it)
- Install all security patches and updates

2.3.1.2. HARDENING CHECKLISTS

A hardening checklist (also known as a lockdown guide) is an important document containing step by step instructions for securing systems. Most vendors provide hardening documentation for their products and are a good starting point.

These resources should be utilised to create a baseline hardening document for the associated system for the SOCIALIZE Consortium. This should be authored by a coalition of resources that have technical expertise in the system being hardened and have security expertise. A point of note is 'less' is 'more' with regards to security.

All deployments should then be configured as per the document. Policy should dictate that if any part of the hardening process is left out, then a business justification for non compliance is raised and documented. All non compliance justifications should be reviewed periodically to ascertain if they are still legitimate.

If there is no existing hardening checklist available for a system from either the vendor or the resources listed above it is advised that suitable security guidance is sought from a professional who has a proven record of expertise in the area to provide assistance in producing one.

2.3.2. PATCHING MANAGEMENT

Patch Management is the ability to implement patches in a timely manner using strategies and plans as appropriate to ensure systems and services continue to be available and secure for the purposes of the business function(s) they provide.

Patch Management is the ability to implement patches in a timely manner using strategies and plans as appropriate to ensure systems and services continue to be available and secure for the purposes of the business function(s) they provide. Patching (sometimes also known as a "fix") is a technique used to correct a problem (often known as a "bug") in a computer program. This is typically done by obtaining a repair program from the vendor which the original computer program was purchased from.

Patches can be summarised into the two categories:

- Functional
- Non-Functional

2.3.2.1. FUNCTIONAL

This typically involves correcting features or functionality of a computer program.

Functional patches may involve changes to the "look and feel" of certain areas of a product or areas that may not work as intended but which do not affect the overall security of the application.

From a purist point of view, it may be noted that functional problems may affect the ability to undertake certain tasks which can align with availability targets. However, security generally would focus on more significant impacts such as complete unavailability e.g. denial of service, or integrity of the computer program rather than reduced functionality.

If a system requires a functional patch in order to increase it's ability (or restore ability if lost following an upgrade or other reason) to undertake certain tasks or efficiencies, it

would be considered good practice to implement this by following Service Management2 disciplines such as Problem and Change Management. Additionally, when patching systems that have clinical use or functionality, the clinical impacts should be considered within a clinical safety assessment or similar methodology.

2.3.2.2. NON FUNCTIONAL

These types of patch are released for several purposes, many of which are security related. The focus of this document will therefore mainly consider these. In the case of patches released to repair or mitigate a specific security vulnerability found in a system in live service. The severity of the vulnerability generally dictates the timescale for availability, ultimately leading to deployment and subsequent correction of the vulnerability. The addition of the patch usually will not affect functionality or have affects to users of systems or services, however, this should be confirmed via pre-deployment testing and/or post implementation testing, where systems have clinical impact or use, appropriate levels of testing rigour should be applied to all patches.

2.3.2.3. UPGRADE

The activity of upgrading a system, i.e. moving to a new release of computer code, may include many previous functional and non-functional patches, while at the same time adding new features or functionality not available previously.

Once an upgrade is available this may negate the need to apply previous non- functional patches. Non-functional patches made available beyond this date should then be applied as and when they are released.

Upgrades may comprise of interim release such as “Services Packs” which complement major releases of Microsoft Windows OS, or a move to a complete major release.

2.3.3. VULNERABILITY DISCLOSURE

For the purposes of of this document, the majority of the content will be focused in respect to Non-Functional patches to potential information security vulnerabilities. These vulnerabilities may be disclosed in a number of ways or not at all. It is important to understand these concepts as they can influence risk management decisions.

Vulnerabilities may be found by various types of individuals, groups and organisations and the methods used to disclose discovered vulnerabilities can vary considerably. It should also be noted that the availability of non-vendor patches or interim fixes may differ between disclosure methods and must be considered fully before any potential implementation.

2.3.3.1. RESPONSIBLE DISCLOSURE

Vulnerabilities disclosed in this way are reported to the vendor(s) of the products concerned. The individual, group or organisation which discovered the vulnerability

works with the vendor to ensure that the vulnerability is satisfactorily resolved. Using a responsible disclosure methodology, no details of the vulnerability are released publicly by either the vendor or the discoverer of the vulnerability until a corresponding patch is made available.

This approach gives a window of opportunity to address the problem and release a patch to the affected communities.

The vendor and the discoverer of the vulnerability both conduct a 'co-ordinated release' of the patch and vulnerability details simultaneously once the patch is available. The discoverer of the vulnerability is credited publicly with discovering the vulnerability by the vendor. For an individual, group or organisation this can be good publicity.

In the last few years, there has been much more of a focus on 'responsible disclosure' for economic reasons. A number of organisations have started paying individual security researchers and groups for 'sole rights' to a newly discovered vulnerability via 'bounty' programmes and then working with the vendor of the affected product on the researcher or groups behalf. This allows researchers and groups to remain 'anonymous' to the product vendor if they so wish but also allows them to get paid for their work.

Previously, many security researchers worked on discovering vulnerabilities in products purely for the intellectual challenge of doing so and without any financial motive. Another argument for such 'bounty' programmes is that they discourage potentially 'less ethical' security researchers from selling discovered vulnerabilities to criminals who would use the vulnerabilities to compromise systems for financial gain.

2.3.3.2. PARTIAL DISCLOSURE

The 'partial disclosure' methodology is characterised by some 'high-level' details of the vulnerability being divulged to the general public. This is often via a security researcher's web site or blog or possibly via one of the well known security mailing lists such as 'Bugtraq'.4 Via this route, the vendor is notified of the vulnerability as well (or is notified directly by the discoverer of the vulnerability) and will often produce a 'security bulletin' detailing some mitigating actions which can be taken prior to a patch being released. If the mitigating actions are followed, they can often lead to a loss of functionality in the product containing the vulnerability. Therefore, a risk assessment should be performed to determine level of exposure to the vulnerability and vulnerability severity versus the consequence of lost functionality for users of the product.

Some security researchers and groups follow the partial disclosure methodology because they feel it encourages the vendor to produce a patch for a vulnerability more quickly than if they notified the vendor directly. On occasions, the security researcher or group will give the vendor a time limit for producing the patch, which if not achieved by the vendor, will see the researcher or group release full details of the vulnerability to the public – potentially creating risks with little or no mitigation immediately available.

2.3.3.3. FULL DISCLOSURE

Security researchers and groups who practice the 'full disclosure' methodology feel that all systems should be open to scrutiny and that information on vulnerabilities in systems should be made available to all. This for example allows customers to determine their level of exposure themselves and put mitigating actions in place without vendor timescales driving these activities. A downside is that by releasing full details to everyone, this information also makes it into the hands of more nefarious individuals.

Vulnerabilities reported in this way are therefore reported to everyone at the same time via either security related mailing lists, security websites or blogs. This provides opportunities for potential attackers to exploit these vulnerabilities before vendors release patches and affected organisations are able to apply them.

Upon discovering vulnerabilities disclosed in this way, a vendor will often produce guidance for customers in the form of a 'security bulletin' which details possible mitigations which can be put in place prior to a patch being released. Note that potential mitigations may involve disabling certain functional aspects of a product. In these instances, a risk assessment should be performed to determine level of exposure to the vulnerability and vulnerability severity versus the consequence of lost functionality for users of the product.

Other mitigations may be possible in the short term before a patch is made available. For example, technologies such as Intrusion Prevention System may assist as interim measures – however, they should not be solely relied upon.

2.3.3.4. NO DISCLOSURE

In some circumstances vulnerabilities are developed often for financial gain. In this scenario an organisation or person may choose to use vulnerability for its own purposes (sometimes illegal) and not make it known to any outside communities.

A slight variation on this theme is that the same organisation or person may choose to auction a discovered vulnerability to the highest bidder. This again could be used for illegal activities, or it may be purchased by the vendor of the system concerned or an intrusion prevention system provider to enhance its own products.

A zero-day (or zero-hour) vulnerability is one that is unknown to both the vendor of the affected product and the general public and for which no security update exists. Zero-day vulnerabilities often receive active exploitation 'in the wild' and exploitation of the vulnerability is often how they are discovered.

2.3.4. WHAT SHOULD BE PATCHED?

2.3.4.1. OPERATING SYSTEMS

Sometimes referred to as OS, this is an interface between hardware and applications; it is responsible for the management and coordination of activities and the sharing of the

limited resources of the computer. Examples of operating systems are Microsoft Windows and Linux.

2.3.4.1. APPLICATION

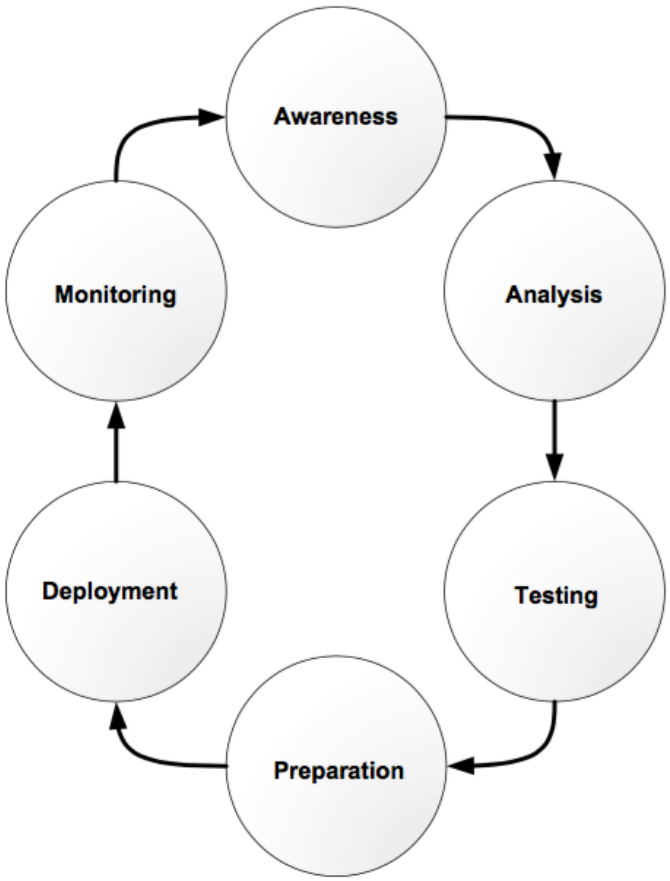
Some applications come included with an OS, while others are added as need arises. Common user applications include Microsoft Office applications and Adobe Acrobat, system applications may include Web servers and Databases.

2.3.4.2. FIRMWARE

These are typically coded instructions that are stored in permanent or semi- permanent memory. An example of this would include a computer BIOS which is loaded prior to an OS or application. Other examples may include the firmware used on network devices or in medical devices that serve important functions.

2.3.5. PATCH MANAGEMENT PROCESS

There are many variants of patch management processes, however typically they include several of the following areas:



2.3.6. SECURING AGAINST VIRUSES, MALWARE AND EMAIL HOAXES

Attackers are increasingly utilising viruses and malware in their attempts to compromise systems, gain unauthorised access to information and to take control of computer resources - often redirecting these resources for attacks against other targets.

Spyware and malware is often bundled with legitimate software. When users install the legitimate software they can also inadvertently install the bundled spyware affecting the confidentiality and integrity of their systems security. .

The nature of this type of software can present long term issues for security because it often remains hidden from the user (or poses as a legitimate application) while continually divulging information from the infected host. The most effective defences against viruses, malware and hoaxes are those that combine various technologies and strategies. These range from in-depth technical solutions to effective user education, preventing the compromise of these technical solutions.

2.3.6.1. ANTI-VIRUS

Anti-virus software and related applications can be used as a technical defence to stop viruses from infecting systems. Such software is generally host based and runs on the system it is protecting. Anti-virus software can detect many types of malware. These types include computer viruses, worms and 'trojan horses' as well as spyware.

A 'computer virus' is a type of malicious software which infects files on a computer system. A virus may look for specific types of file to infect such as Word documents; once an infected document is sent to someone else, the virus then spreads to and infects that persons PC. A 'resident' computer virus can survive system reboots and operates in the background on the system, looking for files to infect. A 'non-resident' computer virus only runs when an infected file is launched.

A 'worm' is a type of malicious software which does not require user interaction to run. Worms can spread from system to system utilising automated infection methods and generally exploit un-patched software vulnerabilities in order to spread. A worm does not steal personal information from systems but simply exists to spread and cause system problems in relation to integrity and availability.

A 'trojan horse' is malicious software which on the surface has a legitimate usage but unbeknownst to the user contains functionality which can be used to steal sensitive data or perform other unwanted actions.

2.3.6.2. MALWARE AND SPYWARE

Due to the many possible methods of infection by malware and spyware, an effective anti-malware strategy requires equally varied levels of protection. Many types of malware application collect information which may be valuable to vendors of those applications, such as browsing habits or the popularity of certain products. This

information can then have resale value to the vendor for marketing purposes and can be sold on to other companies. More sensitive information can also be stolen by such software including credit card numbers, credentials for online banking services (often via a keylogger) and so forth.

Some types of malware once installed can be used to provide a 'remote control' facility to attackers. Once installed, the users system becomes part of a larger group of compromised systems known as a 'botnet'. These botnets are controlled centrally and can be used for a variety of purposes such as the sending of spam e-mail or for performing 'Distributed Denial of Service' (DDoS) attacks on legitimate web sites.

User Education

End user education is one of the most effective tools for the prevention of malware incidents. This should make sure that each user can recognise suspicious behaviour, will not attempt to circumvent technical solutions by installing unapproved software, open suspicious attachments or visit websites designed to spread malware. User education should be an ongoing activity and should begin when an employee joins an organisation. Multiple methods for educating users exist including using posters, desk drops, login banners/notices, formal training sessions and so forth. It is of vital importance that the education links in with the corporate policies on anti-virus, acceptable use and so forth.

User education is a key weapon in preventing malware attacks. Whereas previously, visiting certain types of web site or malicious site could result in attempted infection via malware, there have been a growing number of incidents where legitimate and well known web sites have been used to spread malware due to elements of the sites being compromised.

- The proper policy and procedure regarding malware might include reference to:
- Identifying suspicious attachments.
- The reporting procedure for possible incidents.
- The types of websites which attempt to install malware covertly.

How suspicious behaviour in software can indicate a malware presence.

Technical Solutions

Solutions offering varying levels of protection and monitoring of malware behaviour are widely available. However, due to the covert nature of their existence, detection of new types of malware can be difficult.

Active Monitoring

Active monitoring of user machines provides real time protection against malicious processes. There are various, freely available software products that can actively probe all applications running on a machine which can offer some protection against this type of attack. If an application demonstrates behaviour indicating the presence of malware, this type of software should prevent the application starting.

Active monitoring software should include the following features: • Active process monitoring.

- Signature based detection.
- Behaviour based detection.
- Application/Process quarantine

2.4. SECURING APPLICATION

2.4.1. WEB APPLICATION SECURITY

To measure the security of a system is important to evaluate its potential weak points and evaluate the application vulnerability categories.
These categories are used to illustrate guidance for application developers and architects. With these categories, you can focus consistently on the key design and implementation choices that most affect your application's security.
Application vulnerability categories are listed in Table 1 and are described in detail in the following paragraphs.

Category	Description
Authentication	"Who are you?" Authentication is the process where an entity proves the identity of another entity, typically through credentials, such as a user name and password.
Authorization	"What can you do?" Authorization is how your application provides access controls for resources and operations.
Input Validation	How do you know that the input that your application receives is valid and safe? Input validation refers to how your application filters, scrubs, or rejects input before additional processing.
Session Management	A session refers to a series of related interactions between a user and your Web application. Session management refers to how your application handles and protects these interactions.

Sensitive Data	Sensitive data refers to how your application handles any data that must be protected either in memory, over the wire, or in persistent stores.
Cryptography	How are you keeping secrets, secret (confidentiality)? How are you tamperproofing your data or libraries (integrity)? How are you providing seeds for random values that must be cryptographically strong? Cryptography refers to how your application enforces confidentiality and integrity.
Error Handling	When a method call in your application fails, what does your application do? How much do you reveal? Do you return friendly error information to end users? Do you pass valuable exception information back to the caller? Does your application fail gracefully?
Auditing and Logging	Who did what and when? Auditing and logging refer to how your application records security-related events.

Table 1 : Application Vulnerability Categories

2.4.1.1. AUTHENTICATION

Authentication is a first line of defense. The application must determine if the user is who he/she claims to be or if the entity, a server or program, is what it claims to be.

The most common form of authentication is the user id and password. Authentication policies, processes, and logging must be designed, developed and documented to assure that the application keeps unauthorized users from accessing the site. It must correctly identify the true owner of a user id and password.

The passwords must be protected whilst being stored on application servers and whilst they are transmitted. There are several points during the lifetime of a password which require special attention.

The passwords must be stored in a secure location and encrypted, they must never be transmitted in the clear (i.e. without using protection such as SSL) and never fully visible in account management emails.

Make use of “no cache” tags to further prevent someone from backing up to a login page and resubmitting a logon. Do not allow the application to cache both user id and password. “Remember me” functionality is not recommended

Note on SSL: SSL can provide authentication, confidentiality, and integrity for data as it is transported to and from web services.

Platform checkpoints:

1. To prevent a user id and/or password from being hacked, failed logins should trigger a lock-out after a determined number of attempts. The account lock-out should be maintained for a number of hours to prevent and discourage the attacker from reissuing the attack. The activity should be logged.
2. All authentication attempts should be logged (log in, log outs, failed logins). In addition notification should be sent to an administrator when the account is locked due to failed logins.
3. Strong password rules should be applied. A strong password has a minimum of seven characters and it uses three of the following: numbers, upper case letters, lower case letters, and symbols. A strong password will not use repeated or sequenced characters. It will look random. Finally, the password should not be found in any dictionary. Implement a password expiry time for all passwords.
4. When a password is changed, require the existing password to be entered prior to accepting a new password. It is important to verify that the owner of the user id is the person requesting the password change. When passwords are successfully changed the program should forward a message to the email address of the owner of the user id, and the user should be forced to re-authenticate. When a user forgets a password, the password must be changed rather than "recovered."
5. Passwords should not be stored in a manner that would allow a recovery.
6. Passwords and user ids must be transmitted and stored in a secure manner. Do not send user ids and passwords in a clear-text email message. Should this be a necessity, any passwords sent in clear text must be encrypted using Secure Socket Layer (SSL).
7. Forms based authentication must use a POST request to assure that the authentication credentials are not cached to browser history.

Using SSL on all login pages will accomplish this. Make use of "no cache" tags to further prevent someone from backing up to a login page and resubmitting a logon. Do not allow the application to cache both user id and password. "Remember me" functionality is not recommended.

2.4.1.2. AUTHORIZATION

Authorization ensures that the authenticated user has the appropriate privileges to access resources. The resources a user has access to depend on his/her role.

To develop a security strategy to protect back-end and front-end data and systems is important to define what the authenticated identity can do and the resources that can be accessed.

Objectives of authorization are:

- To ensure only authorized users can perform allowed actions within their privilege level
- To control access to protected resources using decisions based upon role or privilege level

Platform checkpoints:

During the design phase, user roles have been defined based on a "least privilege" model. If a user role will not be modifying data, then the role should not be given any opportunity to edit, delete, or add data to the database. It's also important to determine who will hold the responsibility for assigning users to specific roles.

The administrative functions should only be available to users in the admin group and the standard users must not have the capability to elevate their privileges. The user accounts used for your application should be given the least amount of privileges required for them to function correctly.

The user should not be able to access an unauthorized page by entering the location into the URL. Similarly, a user should not be able to enter a file path into a URL that would allow a user to access and potentially modify a system file.

2.4.1.3. INPUT VALIDATION

This section deals with applications being robust against all forms of input data, whether obtained from the user, infrastructure, external entities or databases.

If you ensure that all of the data received and processed by your application is sufficiently validated you can go along way towards preventing many of the common vulnerabilities being actively exploited by malicious users.

It is important to define what data application should accept, what its syntax should be and its minimum and maximum lengths. This information will allow to define a set of "known good" values for every entry point that externally supplied data could exist.

Two main approaches exist for input validation called whitelisting and blacklisting respectively.

A whitelist will allow you to define what data should be accepted by your application for a given input point, in short you define a set of "known good inputs".

The blacklist approach will attempt to do the opposite by defining a set of "known bad inputs" which requires the developer to understand a wide range of potentially malicious inputs.

Platform checkpoints:

If the server validates all data entering the web application against known good criteria, the chances of successful attack are greatly reduced. The burden of security validation must fall on the server, and hence the application developer, rather than the client.

Client-side validation is often used as a primary validation but should not be used as a security defense.

The use of a common library of field validations can be used to more efficiently and accurately confirm the integrity of the entry data.

Input Validation best practices:

- Apply whitelists: where possible decide what is allowed in the field
- Validate data: type, length, format, and range
- Canonicalise all inputs: this means reducing the data received to its simplest form, the format that the server and database expects. It may be necessary to establish character sets on the server to establish the canonical form that input must take
- Sanitize Input : this can include stripping a null from the end of a usersupplied string; escaping out values so they are treated as literals, and HTML or URL encoding to wrap data and treat it as a literal

As noted in the Authentication section, an SSL connection is established in the transport layer, after the malicious code is introduced. It is important to recognize that SSL does not protect against invalid data.

2.4.1.4. SESSION MANAGEMENT

A common vulnerability of web applications/services is caused by not protecting account credentials and session tokens.

Session management allows application to only require the users to authenticate once and also confirm that the user executing a given action is the user who provided the original credentials. To an attacker any weaknesses in the session management layer of application can be an easy way to bypass the hard work we have done so far in the first three principles.

Attacks against sessions are often focused on obtaining a valid session value through either exploiting your users or taking advantage of weaknesses in the session management functionality itself.

The session values used in application should follow similar principles to the secure password requirements. The session ID's used to identify individual authenticated users should be of a sufficient length to prevent brute force attacks. This length is going to be

determined by the sensitivity of the data or resource we are trying to protect. We do have to stress that session ID length isn't enough to provide protection by itself; you also need to have a high amount of entropy per character in the session ID. A session ID should be constructed from a large character set without any obvious patterns in the ID's.

In this way each user should have a strong session ID that cannot be predicted easily by attackers. It's important now that these ID's are secured both on the application server and whilst they are in transit. The storage location for the session ID's should be a secure location and not in world readable locations, refer to the principle of least privilege we have outlined earlier for guidance on how to secure access to this location. The next point we need to secure is the transmission of the session ID's . If the session ID is transmitted via HTTP it can be easily intercepted and re-used by an attacker, by using HTTPS instead you can protect the session ID in transit.

At this point we should have a session ID that is resistant to prediction, brute force and interception attacks but we do have a few more protection measures to implement before we can be comfortable with the security surrounding our session management. Applications must to verify whether a session ID exists but also must check whether this is a genuine ID.

Platform checkpoints:

Because cookies are transmitted in clear text, the content of the cookie must not contain or be used to obtain sensitive information. State mechanisms were not designed to manage sensitive information. Therefore, state mechanisms should not be used to authenticate users. The user must be made aware of and agree with the use the application will make of cookie sessions.

Session ids should be unique to users, and issued after successful authentication. They should be randomly generated using a respected randomization source. The session id should never contain personal information.

Session ids are always assigned, never chosen by end user. The keyspace of the token must as large as possible to combat guessing and other attacks.

Session ids must be protected throughout their life cycle to prevent hijacking. They should have a time-out set for inactive sessions. Active sessions should also have a set time to expire and regenerate a new session token. This reduces the time window that a hacker would have to break into a session.

Session ids should be protected with SSL. On log out, the session id should be over-written.

2.4.1.5. SENSITIVE DATA

Sensitive data encompasses a wide range of information and can include:

- physical or mental health details
- personal life
- information that relates to you as a consumer or client
- contact information
- birth date and parents' names
- personal address

All of this data belongs to user and needs securing.
There are three essential parts to proper protection of sensitive data.

1. Data Classification: understand what data needs to be protected and create a Data Classification Policy to classify data based on sensitivity.
   At a minimum three levels of data classification are needed:
   - ✓ Restricted: This is the most sensitive data that could cause great risk if compromised. Access is on a need-to-know basis only.
   - ✓ Confidential or Private: This is moderately sensitive data that would cause a moderate risk to the company if compromised. Access is internal to the company or department that owns the data.
   - ✓ Public: This is non-sensitive data that would cause little or no risk to the company if accessed. Access is loosely, or not, controlled.
2. Encryption: Encryption is a very generic term and there are many ways to encrypt data. It's important to implement and manage encryption correctly. The key to a good encryption strategy is using strong encryption and proper key management. Encrypt sensitive data before it is shared over untrusted networks.
3. Secure communication: the importance of protecting specific pieces of information whilst they are in transit and enforce the use of secure transport mechanisms such as SSL

Platform checkpoints:

There are a plethora of steps one can take to secure application's sensitive data from outside threats. Because most of the critical information is stored in databases, it is crucial to implement different database security controls.

- The physical machine hosting a database is housed in a secured, locked and monitored environment to prevent unauthorized entry, access or theft.
- The database software version is currently supported by the open source project, as required by the campus minimum security standards.
- Destination systems (application/web servers) receiving restricted data are secured in a manner commensurate with the security measures on the originating system. All servers and clients meet minimum security standards.
- It should be used secure authentication to the database.
- Restricted data is never sent via email, either in the body or as an attachment, by either users or as an automated part of the system.
- Secure authentication to the database is used and only authorized users have access to the database.
- Restricted data is encrypted during transmission over the network using encryption measures strong enough to minimize the risk of the data's exposure if intercepted or misrouted from database to client workstation.

If there are particularly sensitive information it might be useful to add an additional layer of security and encrypt the extremely sensitive data at field layer.

2.4.1.6. ERROR HANDLING

Errors are inevitable. Errors can be caused by user, programs, or perhaps they are errors between two systems. During development and testing an effort is made to identify all potential errors and appropriate error messages are developed for the end user.

There will also be errors that are unanticipated. The application must have protocols for these errors as well. Left "unhandled," the administrator has no idea that an error has occurred. The procedure for handling the unanticipated needs to include what the error was, when it occurred, and where it occurred.

Platform checkpoints:

During development write a policy for handling errors. Determine which errors should trigger a response to the end user. Carefully write error pages with appropriate information. Decide what the programmatic response will be to known errors. Write error pages that reflect enough information to the end user without giving the user information about the code, the file system, or permissions. When an error occurs that causes the program or a part of the program to fail, it is vital that the system will "fail closed," blocking an unauthorized user from reaching the operating system or the site. The action that caused the error should be logged and then blocked.

2.4.1.7. LOGGING

Logging is crucial to an organization's ability to track unauthorized access and to determine if any access attempt was successful. Logs are vital to reconstruction of events leading to a program failure. Log as much as possible.

Platform checkpoints:

Begin by synchronizing your servers and syslog server to a time server. Time and date stamps must be accurate. Preserve a baseline of your network to be used as a comparison point in the event of system failure.

The following items will make any log entry meaningful:

- Date and Time
- Initiating Process
- Process Owner
- Description

Log all Authentication and Authorization Events – logging in, logging out, failed logins. These should include date/time, success/failure, resources being authorized, and the user requesting the authorization, if appropriate an IP address or location of the Authentication Attempt. Log all Administrator activity. All of it. Log the deletion of any data. Log any modification to data characteristics.

Log files are critical data. They should be encrypted. Develop a procedure for archiving log files.

2.4.2. SOA SECURITY

SOA is an architectural approach which involves applications being exposed as "services". Services in SOA were associated with a stack of technologies which included SOAP and REST. From a security point of view, all of it must be secured to protect the SOA infrastructure against attack.

The vulnerabilities that can be introduced by Web Services are :

- *Injection Flaws*
- *XML Denial of Service Issues*
- *Harmful SOAP attachments*
- *Insecure Communications*

2.4.2.1. INJECTION FLAWS

Injection flaws occur when software does not properly validate input. An attacker could craft malicious input that causes the Web Service software to perform operations on behalf of the attacker. Classes of injection flaws include

1. Cross Site Scripting

   Cross Site Scripting (XSS) attacks occur when an attacker is able to inject a malicious client-side script into a vulnerable web page. When these scripts are run, they can be used to install malicious software on the visitor's computer, steal a visitor's cookie, or hijack a visitor's session.

   Preventing XSS requires separation of untrusted data from active browser content.

2. SQL Injection

   In a SOA, SQL Injection attacks involve the insertion of SQL fragments into XML data to return inappropriate data, or to produce an error which reveals database access information.

   A successful SQL Injection attack in SOA has two prerequisites:

   - Data received by a Service in the SOA is inserted directly into a SQL statement

   - The SQL Statement is run with sufficient privileges to execute the attack.

To counter this attack, it is important to ensure that data received from untrusted users is not directly placed into SQL statements. This can be achieved by enforcing content-validation and threat-detection rules over incoming content.

3. XPath Injection

is analogous to SQL Injection, can be used to "harvest" information from an XML database. XPath injection can be blocked by ensuring that data passed into an XPath expression does not itself contain XPath.

2.4.2.2. XML Denial of Service Issues

This attack exploits a feature of DTDs, namely the ability to pull in entities which are defined in a DTD. By pulling in entities recursively, an attacker can make an XML message which explodes in memory (hence the term "XML bomb") and causes a denial-of-service.

2.4.2.3. Harmful SOAP attachments

Just like email messages, SOAP messages may contain attachments. These attachments may be threatening if they are very large and difficult to process (e.g. a "clogging attack"), or if they harbor viruses. The solution is to ensure that SOAP attachments are

either (a) blocked, (b) filtered based on MIME-type, or (c) passed through a virus scanner.

2.4.2.4. INSECURE COMMUNICATIONS

Use the latest versions of SSL to protect the content of messages in point-to-point transactions. Requiring mutual authentication between the client and server raises the level of trust before processing messages and generally decreases the attack surface of the service. Web Services allow for messages to be routed through multiple intermediaries; one of the intermediaries may terminate the SSL connection so the message may not be protected between all of the intermediaries. In these architectures, use endtoend security mechanisms like XMLEncryption, XMLSignature, and SAML assertions (Security Assertion Markup Language).

2.4.2.5. IDENTITY AND STANDARDS

It is important to know who is using the services of a SOA, and to use this information to control access and to maintain information within an audit trail. The task of controlling access to the services makes use of a variety of standards, some established such as X.509 certificates, and some new such as SAML and WS-Security.

X.509 certificates

X.509 certificates are used in the context of SSL authentication, where a Web Service can prove its identity to a client, or, in the case of two-way SSL, the client also proves its identity to the service. In this case "identity" is amorphous, since Web Services interactions often involve applications talking to applications, without a human being involved. So the "identity" is the identity of an application. And, as is the case in all usage of X.509 certificates, the trust is based on the issuer of the X.509 certificate (a Certificate Authority, often abbreviated to "CA").

As well as SSL, X.509 certificates are often used in the context of digital signatures. XML Signature is a standard which defines how XML data can be digitally signed using the private key which corresponds to an X.509 certificate, so that anyone who holds the signatorys X.509 Certificate can validate the signature.

WS-Security

WS-Security is a newer technology which was standardized in 2004. It builds on what has come before. It defines how XML Encryption and XML Signature apply to SOAP, so that a SOAP message may be encrypted and/or signed. Additionally, it defines where passwords and X.509 Certificates are placed in a SOAP message, and how SOAP may operate with Kerberos. This allows for interoperability between different applications which use WS-Security.

Platforms such as WSO2 incorporate WS-Security. These allow processing of signed XML (using XML Signature with WS-Security), authentication (using passwords or certificates), and encryption (XML Encryption with WS-Security).

XML gateways provide security for SOA by providing security processing on the network, using hardware acceleration. The XML gateway applies security policies to the services in the SOA which it protects. It presents "virtual services" which sit in front of the actual Web Services themselves. These virtual services are accelerated, and may include transformation which occurs before the actual SOA services are called. For example, an XML gateway may present a REST interface in front of an actual SOAP Web Service. In this way, XML gateways often provide protocol mediation, transformation, and acceleration as well as security.

2.5. BIBLIOGRAPHY

Enterprise Security Architecture: A guide to Infosec management

Di Rassoul Ghaznavi-Zadeh

Web application security

http://www.applicure.com/solutions/web-application-security

SANS Institute InfoSec Reading Room

A Security Checklist for Web Application Design

http://www.sans.org/reading-room/whitepapers/securecode/security-checklist-web-application-design-1389

Open Web Application Security Project

https://www.owasp.org/index.php/Top10#OWASP_Top_10_for_2013

Database Hardening Best Practices

https://security.berkeley.edu/resources/best-practices-how-articles/database-hardening-best-practices

SOA Security

http://www.networkworld.com/article/2264806/lan-wan/soa-security--the-basics.html

3. PRIVACY

3.1. INTRODUCTION

The respect for human rights and the individual person has changed profoundly in the last two centuries. Today in principle are no longer endurable slavery and torture, even the death penalty is much criticized by the public in fact a growing number of states are considering to put it outlaw. The public opinion is that the individual must be respected in any situation and context. In the last century the initiatives to establish rules to ensure compliance with the minimum rights of a man have multiplied.

With the new trends of globalization and the introduction of new technologies we must consider new forms of protection. The new world organization, extending the boundaries and the new possibilities offered by technology, has introduced further restrictions to the individual freedom.

The evolution of technology has made possible to increase communication, the ability to store data and the dissemination of digital information. The evolution, although useful to the improvement of life, can however introduce new habits that lack respect towards the human being. Some new possibilities can hide pitfalls not easily undetectable to a gross examination.

With the increase of life expectancy and the consequent increase of the elderly population there has been a social change that has a big impact on the economy, national health organizations and the whole society.

Today there is the need to maintain, or better, to improve the quality of life with new approaches that allow to extend services and assistance for a growing part of the population, without aggravating the health and economic structures.

To achieve this objective, it could be possible to use the remaining capacity of the still active patients and elderly making them work together to find new solutions, so that these people could turn into a resource.

It is necessary to take advantage of the new technologies of Information and Communication Technologies (ICT) that, if applied incorrectly, can become invasive and in contradiction with the individual freedom.

It is therefore necessary to observe the rules of professional conduct that, if ignored, might limit the individual freedom. To this end, we will refer to the numerous declarations and conventions that have formalized, fairly accurately, about human rights and what it is needed to avoid violating the individual freedom.

The right to privacy should not be confused with the right to secrecy. Even the right to secrecy is designed to protect an area reserved for private life. Secrecy, in respect to privacy, includes the element that information are for some reason known by some

people. For example, the doctor is certainly aware of the state of health of the patient, but has a duty to maintain the confidentiality of the information in his possession.

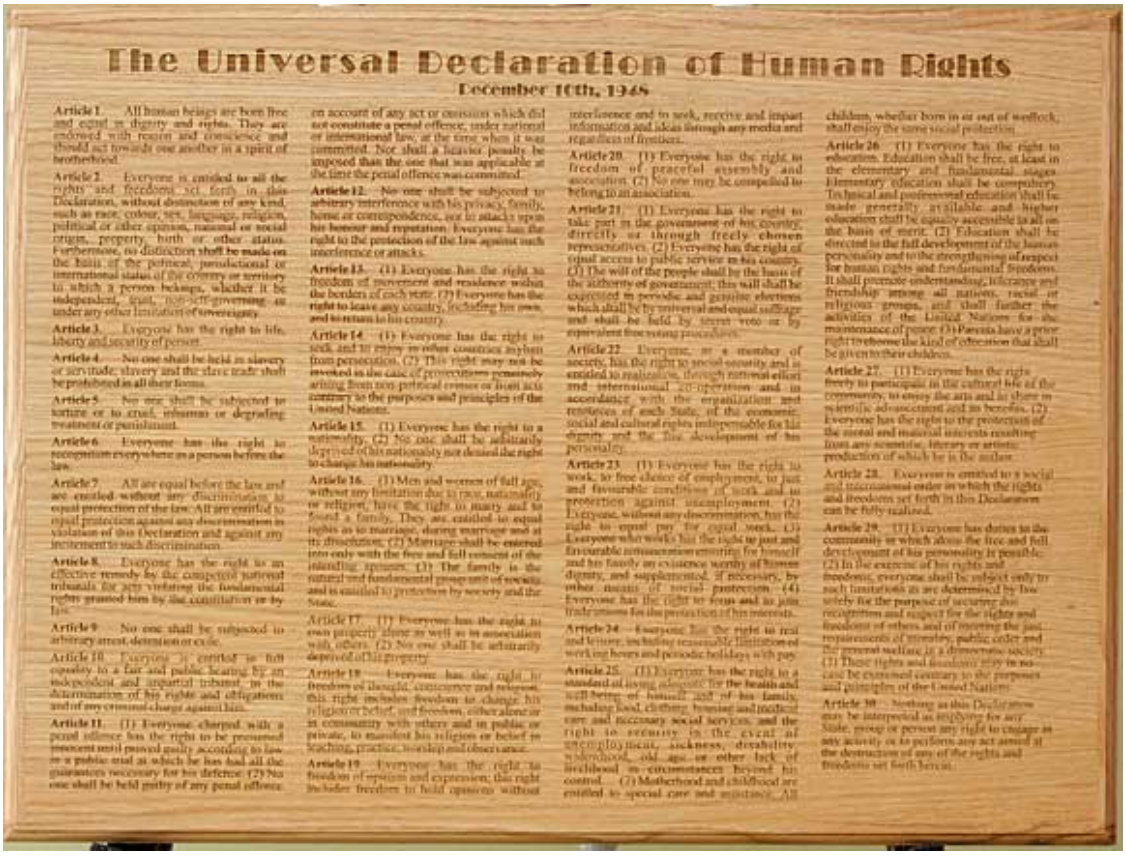
Privacy should not be confused even with loneliness, because there is a profound difference, indeed, between “being alone” and “being left alone”.

3.2. THE CONCEPTS OF ETHICS AND INDIVIDUAL FREEDOM

In a globalized society, the right to information and privacy must be legally regulated not only domestically but also internationally. This paper reviews the principles of ethics and individual freedom and their evolution over time. Particular attention has been made on the rights of the elderly considered a weak category and for this they are often ignored.

3.2.1. THE EVOLUTION OF THE CONCEPTS OF ETHICS AND INDIVIDUAL FREEDOM

On December 10, 1948 the General Assembly of the United Nations issued a statement consisting of a preamble and 30 articles, called "The Universal Declaration of Human Rights" (Figure 1 and Figure 2), as a result of the experiences of World War II.



The Universal Declaration of Human Rights

December 10th, 1948

Article 1. All human beings are born free and equal in dignity and rights. They are endowed with reason and conscience and should act towards one another in a spirit of brotherhood.

Article 2. Everyone is entitled to all the rights and freedoms set forth in this Declaration, without distinction of any kind, such as race, colour, sex, language, religion, political or other opinion, national or social origin, property, birth or other status. Furthermore, no distinction shall be made on the basis of the political, jurisdictional or international status of the country or territory to which a person belongs, whether it be independent, trust, non-self-governing or under any other limitation of sovereignty.

Article 3. Everyone has the right to life, liberty and security of person.

Article 4. No one shall be held in slavery or servitude; slavery and the slave trade shall be prohibited in all their forms.

Article 5. No one shall be subjected to torture or to cruel, inhuman or degrading treatment or punishment.

Article 6. Everyone has the right to recognition everywhere as a person before the law.

Article 7. All are equal before the law and are entitled without any discrimination to equal protection of the law. All are entitled to equal protection against any discrimination in violation of this Declaration and against any incitement to such discrimination.

Article 8. Everyone has the right to an effective remedy by the competent national tribunals for acts violating the fundamental rights granted him by the constitution or by law.

Article 9. No one shall be subjected to arbitrary arrest, detention or exile.

Article 10. Everyone is entitled in full equality to a fair and public hearing by an independent and impartial tribunal in the determination of his rights and obligations and of any criminal charge against him.

Article 11. (1) Everyone charged with a penal offence has the right to be presumed innocent until proved guilty according to law in a public trial at which he has had all the guarantees necessary for his defence. (2) No one shall be held guilty of any penal offence on account of any act or omission which did not constitute a penal offence, under national or international law, at the time when it was committed. Nor shall a heavier penalty be imposed than the one that was applicable at the time the penal offence was committed.

Article 12. No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.

Article 13. (1) Everyone has the right to freedom of movement and residence within the borders of each state. (2) Everyone has the right to leave any country, including his own, and to return to his country.

Article 14. (1) Everyone has the right to seek and to enjoy in other countries asylum from persecution. (2) This right may not be invoked in the case of prosecutions genuinely arising from non-political crimes or from acts contrary to the purposes and principles of the United Nations.

Article 15. (1) Everyone has the right to a nationality. (2) No one shall be arbitrarily deprived of his nationality nor denied the right to change his nationality.

Article 16. (1) Men and women of full age, without any limitation due to race, nationality or religion, have the right to marry and to found a family. They are entitled to equal rights as to marriage, during marriage and at its dissolution. (2) Marriage shall be entered into only with the free and full consent of the intending spouses. (3) The family is the natural and fundamental group unit of society and is entitled to protection by society and the State.

Article 17. (1) Everyone has the right to own property alone as well as in association with others. (2) No one shall be arbitrarily deprived of his property.

Article 18. Everyone has the right to freedom of thought, conscience and religion; this right includes freedom to change his religion or belief, and freedom, either alone or in community with others and in public or private, to manifest his religion or belief in teaching, practice, worship and observance.

Article 19. Everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers.

Article 20. (1) Everyone has the right to freedom of peaceful assembly and association. (2) No one may be compelled to belong to an association.

Article 21. (1) Everyone has the right to take part in the government of his country, directly or through freely chosen representatives. (2) Everyone has the right of equal access to public service in his country. (3) The will of the people shall be the basis of the authority of government; this will shall be expressed in periodic and genuine elections which shall be by universal and equal suffrage and shall be held by secret vote or by equivalent free voting procedures.

Article 22. Everyone, as a member of society, has the right to social security and is entitled to realization, through national effort and international co-operation and in accordance with the organization and resources of each State, of the economic, social and cultural rights indispensable for his dignity and the free development of his personality.

Article 23. (1) Everyone has the right to work, to free choice of employment, to just and favourable conditions of work and to protection against unemployment. (2) Everyone, without any discrimination, has the right to equal pay for equal work. (3) Everyone who works has the right to just and favourable remuneration ensuring for himself and his family an existence worthy of human dignity, and supplemented, if necessary, by other means of social protection. (4) Everyone has the right to form and to join trade unions for the protection of his interests.

Article 24. Everyone has the right to rest and leisure, including reasonable limitation of working hours and periodic holidays with pay.

Article 25. (1) Everyone has the right to a standard of living adequate for the health and well-being of himself and of his family, including food, clothing, housing and medical care and necessary social services, and the right to security in the event of unemployment, sickness, disability, widowhood, old age or other lack of livelihood in circumstances beyond his control. (2) Motherhood and childhood are entitled to special care and assistance. All children, whether born in or out of wedlock, shall enjoy the same social protection.

Article 26. (1) Everyone has the right to education. Education shall be free, at least in the elementary and fundamental stages. Elementary education shall be compulsory. Technical and professional education shall be made generally available and higher education shall be equally accessible to all on the basis of merit. (2) Education shall be directed to the full development of the human personality and to the strengthening of respect for human rights and fundamental freedoms. It shall promote understanding, tolerance and friendship among all nations, racial or religious groups, and shall further the activities of the United Nations for the maintenance of peace. (3) Parents have a prior right to choose the kind of education that shall be given to their children.

Article 27. (1) Everyone has the right freely to participate in the cultural life of the community, to enjoy the arts and to share in scientific advancement and its benefits. (2) Everyone has the right to the protection of the moral and material interests resulting from any scientific, literary or artistic production of which he is the author.

Article 28. Everyone is entitled to a social and international order in which the rights and freedoms set forth in this Declaration can be fully realized.

Article 29. (1) Everyone has duties to the community in which alone the free and full development of his personality is possible. (2) In the exercise of his rights and freedoms, everyone shall be subject only to such limitations as are determined by law solely for the purpose of securing due recognition and respect for the rights and freedoms of others and of meeting the just requirements of morality, public order and the general welfare in a democratic society. (3) These rights and freedoms may in no case be exercised contrary to the purposes and principles of the United Nations.

Article 30. Nothing in this Declaration may be interpreted as implying for any State, group or person any right to engage in any activity or to perform any act aimed at the destruction of any of the rights and freedoms set forth herein.

Figure 1: The Universal Declaration of Human Rights

Article 12 of the Universal Declaration of Human Rights proclaims that "no one shall be subjected to arbitrary interference with his privacy, family, home or correspondence,

nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against interference or attacks longer available".

On April 11, 1950 was signed in Rome the "Convention for the Protection of Human Rights and Fundamental Freedoms". The text was drafted in French and English. These are the only versions that are considered to be originals.

The agreement was signed by twelve countries that were then part of the Council of Europe (Belgium, Denmark, France, Greece, Ireland, Iceland, Italy, Luxembourg, Norway, Netherlands, United Kingdom, Sweden) and entered into operation in 1953, with the exception to Italy where he came into enactment in 1955. On June 22, 2007, the Convention has been ratified by all current 47 member states of the Council of Europe (Belgium, Denmark, France, Ireland, Italy, Luxembourg, Norway, Netherlands, United Kingdom, Sweden, Greece, Turkey, Iceland, Germany, Austria, Cyprus, Switzerland, Malta, Portugal, Spain, Liechtenstein, San Marino, Finland, Hungary, Poland, Bulgaria, Slovenia, Lithuania, Estonia, Czech Republic, Slovakia, Romania, Andorra, Latvia, Albania, Moldova, Macedonia, Ukraine, Russia, Croatia, Georgia, Armenia, Azerbaijan, Bosnia and Herzegovina, Serbia, Monaco, Montenegro). During the years, the convention has had several amendments and addition of contents with the modification of its primary goals.

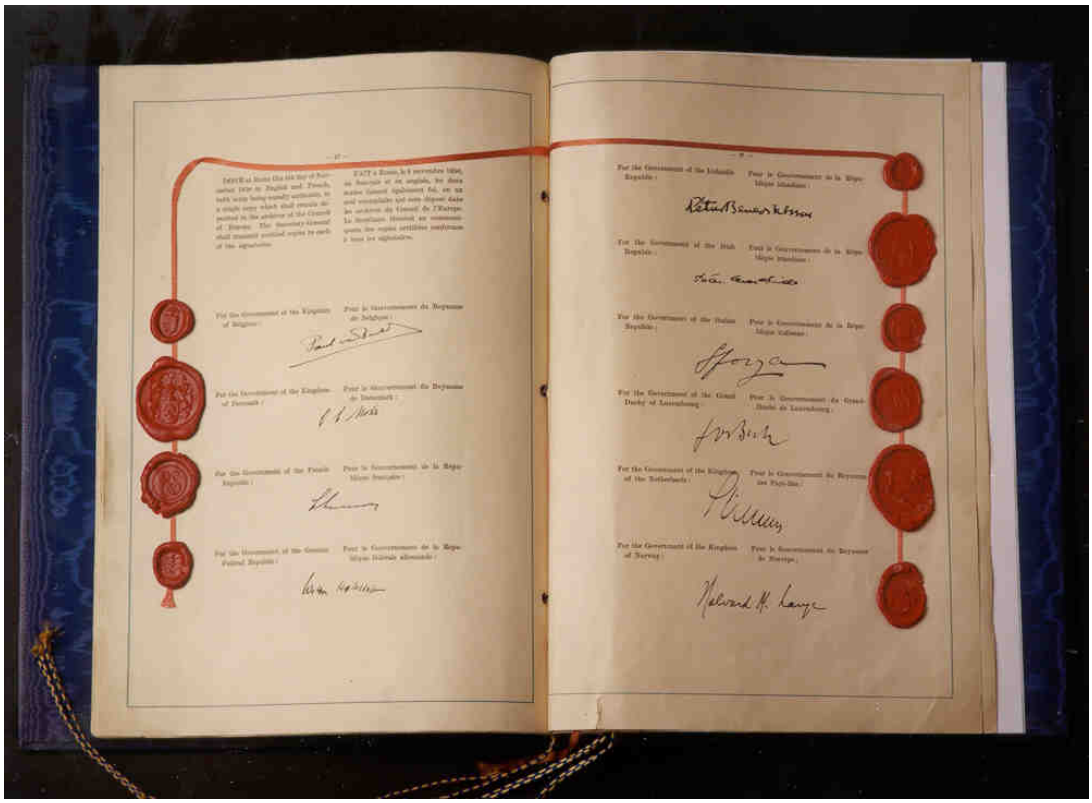


Figure 2: European Convention on Human Rights, initially signed in 1950. (Photo: European Commission)

On December 7, 2000 in Nice, the European Parliament and the Council and the Commission solemnly proclaimed as the Charter of Fundamental Rights of Europe, a text that called "Charter of Fundamental Rights of the European Union" composed of 54 items. The evolution of this document has accentuated the need to safeguard the privacy and dissemination of personal data.

More explicit, as well as technically evolved and advanced, is the rule formulated at European level on the article nr. 8:

1. everyone has the right to protect the personal data concerning himself;
2. such data must be treated fairly for specified purposes and with the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right to access data collected concerning himself, and the right to have them rectified;
3. compliance with these rules is subject to the control by an independent authority.

This implies the creation of a figure that is responsible for the processing of personal data who will be the custodian and guarantor of them. An independent authority should exercise the control and provide assurance that data processing is carried out only for legitimate uses. The rule is part of the role and the role is played by that person that the social system recognizes and appreciates. In the European scenario this person is called "Privacy Officer" and has the functions of responsibility. The challenge of this organism is the ability to professionalise the internal function of privacy protection.

Figure 3: European Data Protection Supervisor logo

It was therefore created an authority called "*EDPS: European Data Protection Supervisor*" (Figure 3, Figure 4) that is an independent supervisory authority devoted to protecting personal data and privacy and promoting good practice within the institutions and organs of EU.

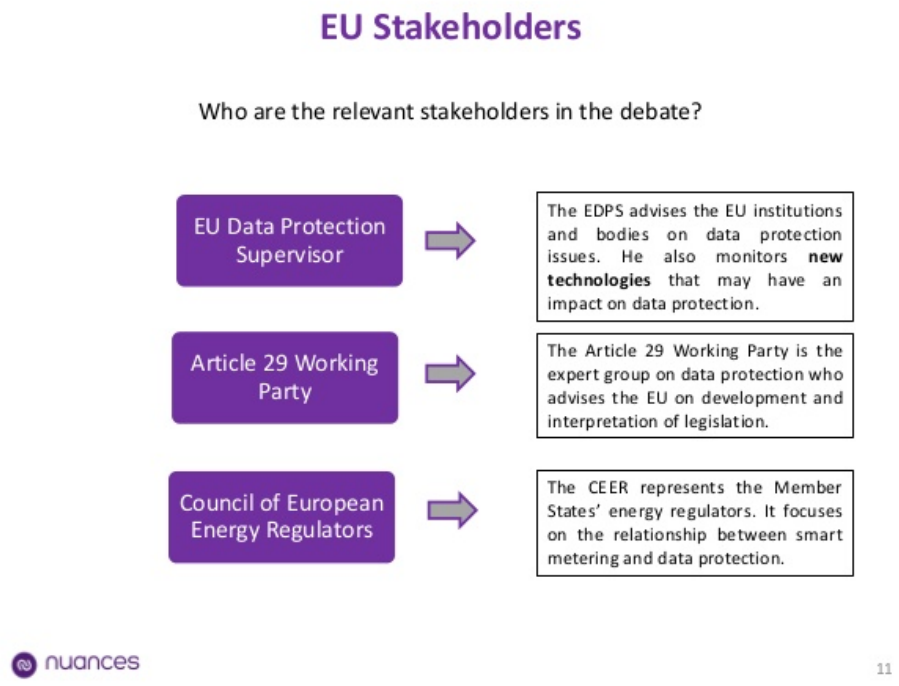


Figure 4: Relevant Stakeholders in EU

The European Union has set up a legal and judicial system concerning the protection of privacy that has encouraged many Member States to introduce new institutions.

The main guidelines of the European Council regarding privacy are:

- Directive 95/46: protect the individuals with regard to the processing of personal data and on the free movement of data.
- Directive 97/66: processing of personal data and protection of privacy in the telecommunication sectors.
- Directive 2002/58: the processing of personal data and protection of privacy in the electronic communication sectors.

First two directives introduce the concept of consent and the right to decide not to appear in the telephone and to maintain anonymity in calls.

The latter Directive provides for freedom of movement of personal data within the EC and prohibits all forms of interception of communications and related data, without the express consent of those concerned or legal authorization.

Member States must ensure fair processing of data by communicating in advance the purpose of the collection and the treatment, the accuracy, the update and the storage for a period no longer than the necessary to achieve the purpose.

In recent years, the respect of the ethical principles relating to the research and to the development of ICT is still growing in importance and the European Parliament has determined that the funded researches must respect fundamental ethical principles, including those contained in the "Fundamental Rights of the European Union" .

Proposed projects must present constraints of security, privacy and certification, it is necessary to prepare a report on the "Prior assessment of risks and identification of precautionary actions proportional to the potential risk / damage" to be submitted to the European Advisory Group for “Ethics in Science and New Technologies (EGE) that provides for the exclusion for who contravene the basic rules of ethics.

The rules to follow are formalized in the 7th Framework Programme (FP7)and are reported in the "Ethical Guidelines for Undertaking ICT research in FP7" to participate in the financing proposals. The EU pursues the direction of the society to be involved in the research for scientific and technological progress, in accordance with the common basic principles. The principles have to be observed with regard to the dignity, freedom, equality, solidarity, justice and the rights of citizens.

Research on ICT can raise ethical questions due to its pervasive and ubiquity nature. The progress of ICT science may arise privacy and the researchers who are finding new solutions will have to be very careful.

The right to privacy is now recognized as the right to identity (Figure 5) and to the protection of information. Privacy is the way to defend the integrity of individual identity.

Today, the danger is the mechanism of the new alienation of the modern world. The trend towards globalization of interpersonal relations and of its network of propagation, are seriously endangering the capacity and ownership of the right to identity.

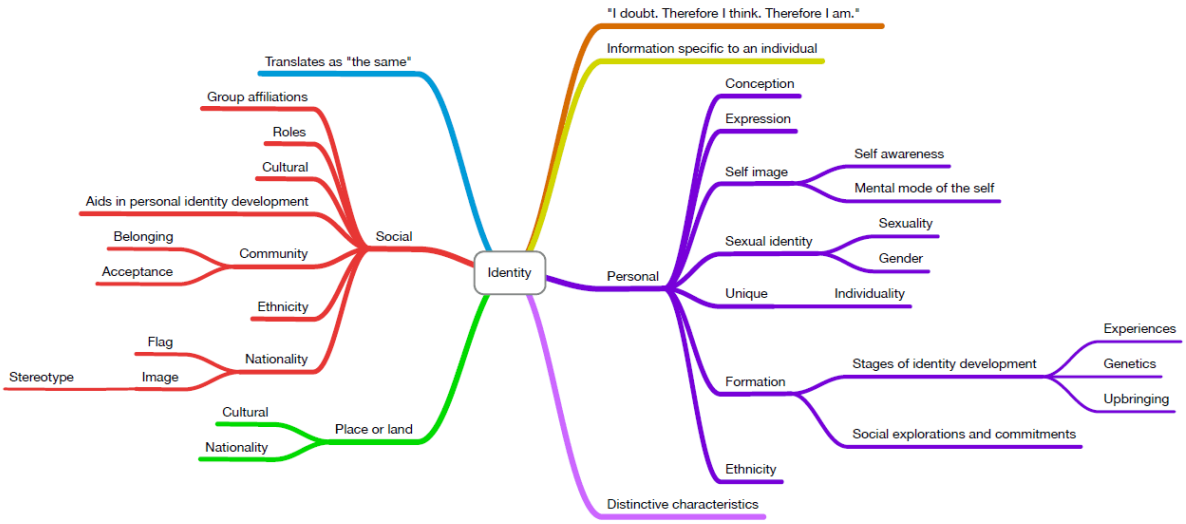


Figure 5: Identity diagram

The centrality of privacy and ethical issues in e-inclusion was further strengthened.

Solutions can bring benefits only if ethical and psychological issues of ICT are properly addressed. However, there is no specific reference point for ethics in ICT for aging, especially regarding the safeguarding of human dignity and autonomy.

During FP7 were organized meetings that have produced many notices about PET, RFID, the 2010 e-inclusion, etc., that have indicated the need to encourage the ICT research oriented towards social goods and to consider as fundamental the values of the European Union.

The main produced publications and meeting where:

- "Science and Society Action Plan", published in December 2001: in this publication is argued that it is *necessary to strengthen the basis of scientific and technological activities, to identify and assess the risks of the progress, and to manage them responsibly on the basis of past experience*.
- Meeting on June 11-13, 2006 hosted by the Government of Latvia in Riga on the theme "*ICT for an inclusive society*": the event included an informal meeting between the Ministers of the EU Member States, the candidate countries, the European Free Trade Area (EFTA) countries and other countries adopted a Declaration on e-inclusion, commonly known as the "Riga Declaration" that explicitly requires the awareness of ethics. The declaration explicitly specifies that particular attention should be paid to further improve user's motivation towards the use of ICT, as well as the confidence through better security and privacy protection. It also declares that in the information society remains a key objective to achieve a better quality of life, and for the autonomy and safety of people, while respecting privacy and ethical requirements.

  Brussels, November 8, 2007 - European i2010 initiative on e-Inclusion titled "*To be part of the information society*": it states that "*it is important to raise awareness of the risks related to the processing of personal data through ICT networks and train users in this area, such as the risk of identity theft, discriminatory profiling or continuous surveillance*".

3.3. THE TERM "PRIVACY"

(Overview of Legislative Decree no. 196/2003)

The term “privacy” is entered in the common language. It is not uncommon to find people of all ages and / or social class who speak about privacy in terms of "... *have violated my privacy*...", "... *my information is protected by the privacy*...". These sentences are all expressions that become widely used.

The interesting aspect is that anyone who uses the term "privacy" thinks in a particular meaning. For someone privacy stands for confidentiality, for other means protecting information that are personal data, or it is the expression of dignity, or even of decency, reputation, etc.

The difficulty of unifying the concept of privacy is the basis of the decision to don’t translate the word "privacy" (Figure 6).

For example, the meaning of "privacy" relates the idea of a right related to personal identity, but this does not exhaust all the aspects of the law relating to individual self-determination.

Figure 6: Examples of desired protection

The meaning of privacy has evolved over time in relation to the technological developments. Originally, the term referred to the sphere of private life but only in recent decades has evolved significantly. Today in fact, the term refers to the right to control over their personal data and to verify that the information is treated or watch by others only when necessary.

Ensuring data privacy means to put in place mechanisms that limit the information that can be acquired and that release information without giving the possibility to identify the specific properties of a user or organization.

To ensure the privacy of the data should not only be consider the technological aspects. The issues of privacy should be regulated at the legislative level.

An example is the new edge technologies that enable the development of applications of public interest, but that can lead to violations of privacy.

With the Ubiquitous computing applied to the care of the elderly, it is possible to have devices that communicate user habits and movements with the surrounding infrastructure. This can lead to violations of privacy, in fact the movement of the person results in what he does, where he is located at a given time etc., acting so a continuous user monitoring.

Unfortunately, the concept of privacy is also abused and someone confuses the concept of *personal data*, which are the basis of individual freedom, with the *public data*, like the budgets of public authorities, the accounts of companies, working hours and salaries of public administration, etc. The concepts of privacy are also felt as that they should not be applied when they come from "public" characters (politicians, civil servants, etc.), even when they commit private actions that could compromise public safety or the economy of the community. Even actions that contravene the laws of the states, when there is the firm evidence, they should not be covered by privacy policies. There are also many discussions about what is right to protect about the secrecy of bank data of people. Although many people give personal interpretation to the meaning of privacy, nowadays it is well known by most of the population. In the following, we will describe the rules that determine when and how to apply the concept of privacy and its limitations.

The common idea is that the privacy concerns the protection of personal and sensitive data. In modern times, the ability to spread data using the computer and the network is very common. Just consider the social networks that spread many personal data, but also video surveillance which involves the handling of images, and biometric systems which allow you to control the "identity of a person", analysing fingerprints or iris scans. Current discussions between EU and some network providers and operators of social networks (Google, Facebook, etc.) fascinate a wide audience.

But, then, what is meant by the word "privacy"?

The concept of privacy is not so much recent. We may recall here the article "Harvard Law Review" by Samuel D. Warren and Louis D. Brandeis, "The Right to Privacy" - BOSTON, December, 1890.

In Europe, when the concept was considered by the institutions, it was used the expression “data protection” (Figure 7), focusing on the significance of the data control. So, with the expression “data protection”, in Europe we find a concept of privacy different from the meaning given in America. The right to privacy on personal data

includes also information that are not connected to the personal sphere, that are the data that we call "common data". The EU adopted in 1995 a directive on data protection (Data Protection Directive 95/46/EC) on the protection of individuals with regard to the processing of personal data and on the free movement of such information.

Figure 7: Data protection elements

This directive provides some definitions that are useful and effective for a greater understanding of the subject. Today, protect privacy means controlling the treatments to which the data are subjected. The processing and dissemination of the data are therefore at the centre of the regulatory system.

On January 25, 2012, the European Commission has presented its proposal for the “EU General Data Protection Regulation” that will replace the “Directive on Data Protection”.

It defines a framework that aims to find a balance between a high level of protection of the privacy of individuals and the free movement of personal data in the European Union. To do that, the directive sets strict limits on the collection and use of personal

data and the delegate each Member State to establish an independent national plan for the protection of such information.

3.4. ELDERLY AND TECHNOLOGY

The trend of increased use of computers and Internet among the over-60 is certainly a fact to be reckoned with.

ISTAT (*National Institute of Statistics of Italy*) statistics report that the use of computers among the elderly between 60 and 64 increased from 13.8% in 2005 to 25% in 2009 and from 5.5% to 9.9% for the group 65-74.

Over the same period the use of Internet increased from 10.8% to 22.8% for 60-64 years old and from 3.9% to 8.5% for 65-74. Just among the elderly, in just four years, there was the biggest increase for use of new technologies. The PC users of 60-64 were up by 81%, that is, the highest increase among all age groups.

There are many reasons and practical needs related to everyday life under this increase. There is to consider the fact that an increasing part of individuals who are approaching old age have a higher education degree.

The ISTAT estimated that in 2050 elderly over 60 will be 38.9% of the population.

The new seniors live in their own age range and ask for help to the technology for their success.

The elderly are the population group that takes greater advantage of the digitization of the activities of everyday life. Increasingly, the elderly want to be active, vital and protagonist of our society.

Information and Communication Technologies (ICT) and Internet gradually pervade exchanges of daily life. This makes possible expanded access to services and opportunities to interact with others and with things that at a previous time would have been unthinkable.

Even companies are beginning to take an interest in the market segment of the elderly population, producing and placing on the market ad hoc devices.

For example the Italian company “Vegan Solutions” has already put on the market a PC with the “Eldy” software. Eldy is an application that includes a set of simplified version tools for seniors able to permit them to use Internet services.

Eldy is developed by a non-profit organization and it is studied for elderly. Eldy is a software applicable to all types of PC and allows using the computer in an easy and intuitive way. The desktop is simplified in six buttons and all the notices are in Italian or in any supported language. Buttons bring intuitively to the use of email, of Internet, of chat, of documents, of video, of saw-connection to TV and photos. The software can be downloaded for free from www.eldy.org and received a European award.

3.5. PRIVACY AND E-PARTICIPATION

E-participation is a key concept in e-inclusion, in particular with regard to the digital divide linked to age. E-participation includes the vote, the opportunity to participate in democratic life, and learning and/or teaching to fit into society and to interact with others. In its broadest sense, the right to participation refers to participation in public life, in what Habermas defined as the "public sphere", which includes the activities of civic associations, neighbourhood groups, social movements and social clubs .

In other words, the domain of action of the public sphere should not be limited to political institutions, but should also include a range of activities including social networks.

The right to public participation is clearly defined in “1948 Universal Declaration of Human Rights” and “International Covenant on Civil and Political Rights”.

Every citizen has the right and the opportunity, without distinctions and unreasonable restrictions “*to participate in the management of public affairs, directly or through freely chosen representatives*”. To do that, *Communication and Information Technology* (*ICT*) plays an important role. It can furnish to citizens more information and more effective communication that are needed for an higher sense of belonging to European community.

Some of possibile example where ICT can just now contribute in everyday life are:

- to remedy to the shopping at the supermarket that can sometimes be exhausting for the heavy packs of water to carry, by placing an order over the Internet;
- the reading activity of newspapers with characters that are often too small, can be replaced reading online the news using customizable fonts;
- to call the children can be used a VOIP software like *Skype* that allows free video calling and therefore the communication can be even cheap and satisfying;
- to monitor elderly health status or benefit from the digital services offered by health care providers, such as online booking of visits or tests and downloading reports.

These and other motives of daily life clarify the growing interest among elderly over 60 toward the new technologies, computers and the Internet!

The right to participate involves three main points: *transparency* (decisions are to be taken as clear), *information* (relevant information should be available free of charge) and *reasoned decision*. At least two of these three elements, transparency and

information, can be facilitated through the adoption of information and communication technologies.

The principle has been reiterated by the preparatory e-participation action, and at the end of the program of e-government.

A major ethical problem, however, is the way in which the e-inclusion is used with regard to the tension between public and private sphere. The concept of e-inclusion certainly emphasizes the importance of being included in families, groups, communities and networks, but also emphasizes the importance of being an independent individual, someone who has the ability to "move away" from intrusion of others.

In fact, between the values of protection under European law recognizing human rights, together with the right to participate, there is respect for privacy and protection of personal data (Figure 8).

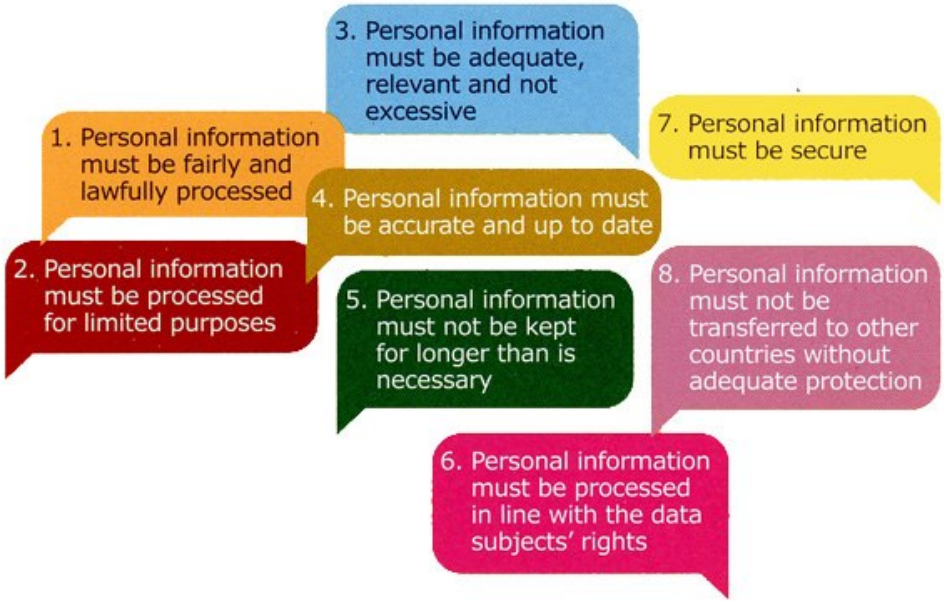


Figure 8: How Personal information must be

Near to the right "'to be left alone" (Figure 9), the right to privacy and data protection have evolved to include a positive function. The positive function is double. The first function is linked to the obligation, for third parties, such as the state authorities or service providers, to enable the individual *to control access to information about him or herself*. Without such a positive element, the protection of privacy of individual cases is not effective, it is purely formal.

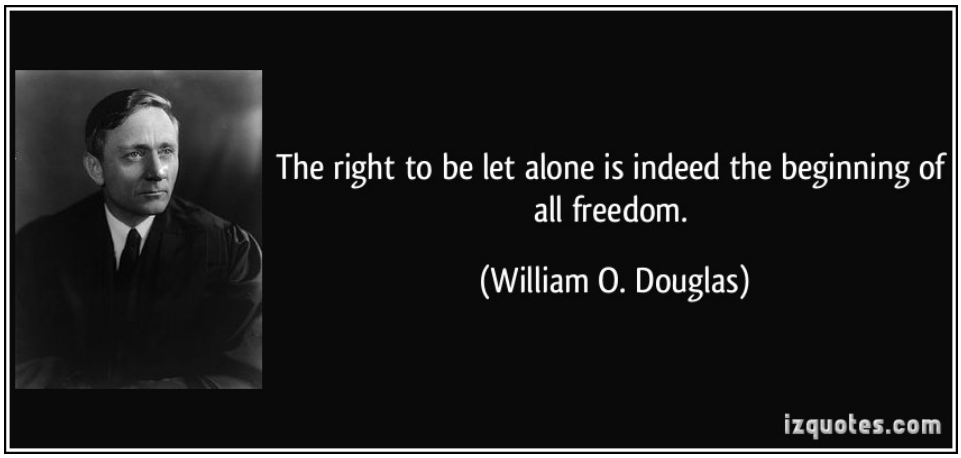


Figure 9: William O. Douglas's citation

The other feature of the positive function of the privacy concerns the construction of a single public sphere and the importance of building individualized relationships. The purpose of this function is to enable the individual to develop his own personality within a network of other human individuals.

If a person is prevented to exchange private e-mails at work, or people receives only news suitable to it's own profile, the perception of others and the world is severely limited. Under these conditions, individual privacy is in danger. If you do not engage in social relationships, people risk to comply with the dominant view. So, people who are afraid of reprisals, prefer to remain silent.

This would be detrimental to individual privacy, as well as the diversity and pluralism, which are pillars of democratic rule of law. Privacy policy, therefore, must also consider *the right to establish and develop relationships with other human beings* and, consequently, to create favourable conditions for this purpose.

European data protection and privacy law protects the individual's ability to obtain and maintain control over ICT (Figure 10) and in particular, over the flow of information that ICTs generate. In addition, the legal values and assets that the rights to privacy and data protection protect go beyond the individual sphere.

The capabilities of modern technology growing at a breath-taking pace, privacy and data protection can be seen as a constitutive value that protects the participation and association in a free society.

From an ethical point of view, the elderly should be protected from the negative consequences of ICT as regards the personal and social rights of the individual. ICT should empower them with the means to protect and pursue their rights. This, however,

may not be enough. Modern technologies should also ensure that the elderly are not isolated, to have a real access to other people or networks of people.

In this light, a legal analysis and ethics should review the requirements and values such as choice, coherence, consensus, confinement, context, adoption, guardianship, transparency and so on, to meet the specific needs of senior citizens.

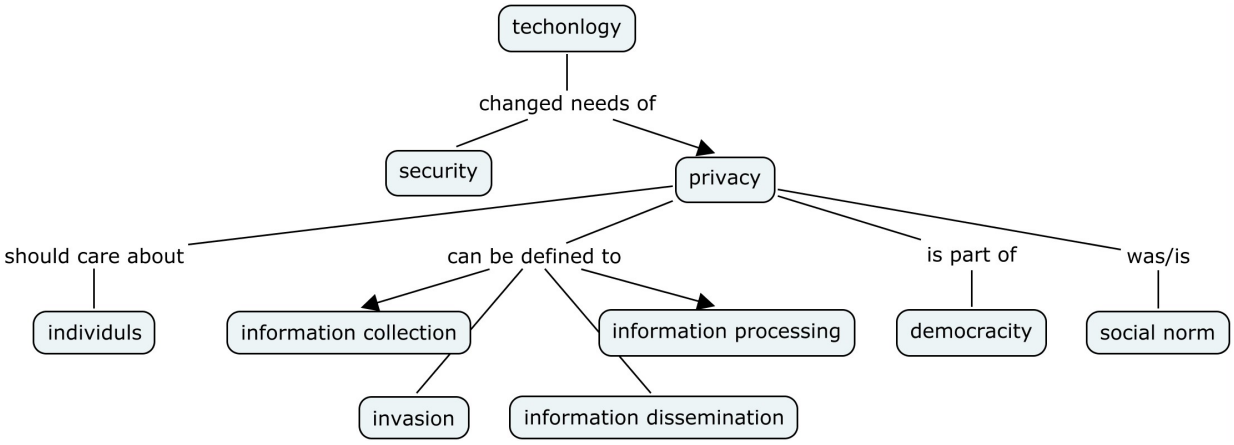


Figure 10: ICT needed changes

3.6. TYPES AND DATA GATHERING AND PROCESSING

The directive 95/46 / EC of 2003 (Figure 11) lays down how personal data should be collected, processed by automated systems (e.g. a database of clients) and how the contained information on them should be archived.

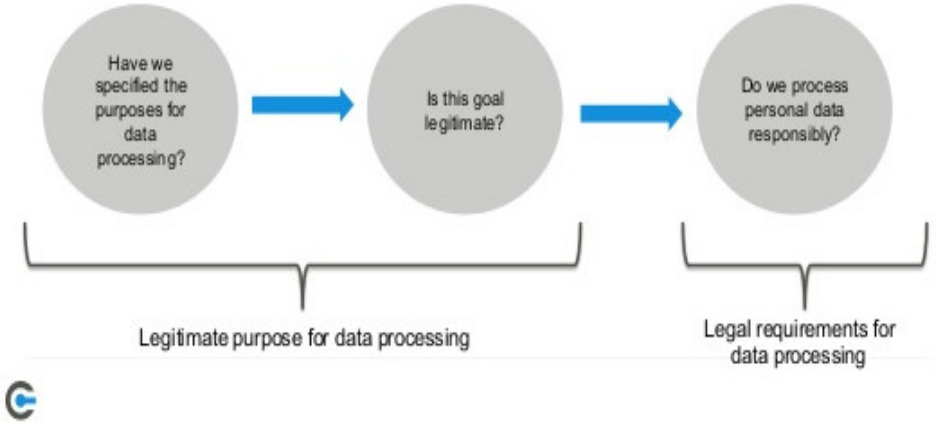


Figure 11:Structure and logic of EU data protection law (95/46/EC)

The rules on data protection are not applied to the following cases:

- by a natural person in the course of a purely personal affairs;
- in the course of activities which fall outside the scope of Community law, such as operations concerning public security, defence or national security.

The Directive aims to protect the rights and freedoms of individuals with regard to the processing of personal data by laying down guidelines determining when this processing is lawful. The guidelines include:

- *quality of the data*: personal data must be processed fairly and lawfully, collected for specified, explicit and legitimate purposes. They must also be accurate and, where necessary, updated (Figure 12);

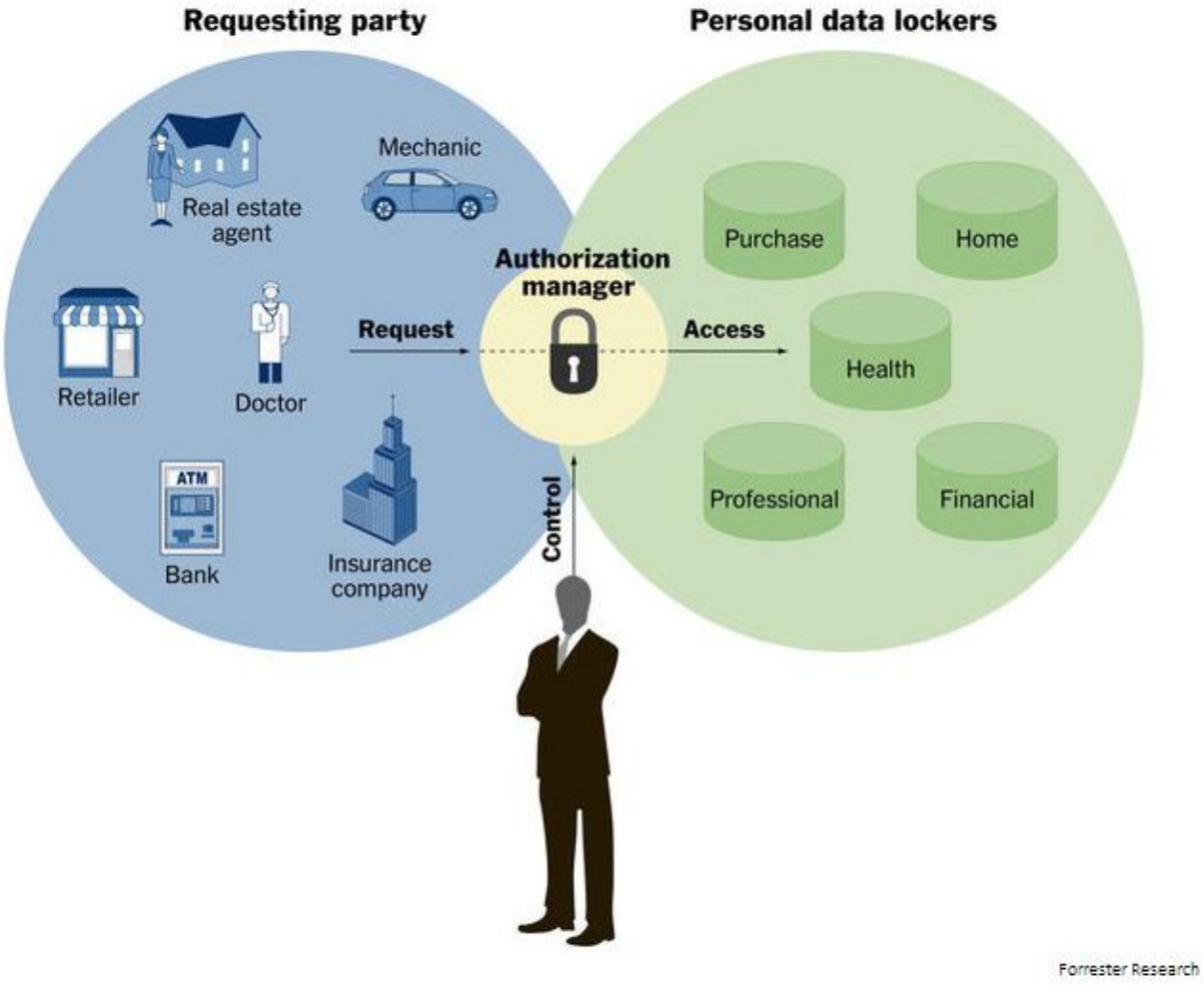


Figure 12: A chart by Forrester Research that envisions a system where consumers would store personal information

- *legitimacy of data processing*: the data may only be processed if the subject has given consent or if processing is necessary for:
  - the execution of a contract to which the subject is party;
  - compliance with a legal obligation to which the controller is subject;
  - protect the vital interests of the subject;
  - the performance of a task of public interest;
  - legitimate interests pursued by the controller;
- *particular categories of processing*: it is forbidden to process personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, and the processing of data concerning health or sex life (Figure 13). This provision comes with certain requirements, for example, in cases where it is necessary to protect the vital interests of the subject or for the purposes of preventive medicine or diagnosis;

- *information to be provided to the subject*: the controller must provide to the subject from whom data are collected with certain information relating to himself/herself (the identity of the controller, the purposes of the processing, recipients of the data, etc.);

Figure 13: Special categories of personal data

- *the subject's right of access to data*: every subject should have the right to obtain from the controller:
    - the confirmation of the existence of data relating to the person when they are being processed and communication of the data that are being processed (Figure 14);
    - the rectification, erasure or blocking of data where the processing does not comply with the provisions of this Directive, in particular, both for nature incomplete or inaccurate data, and the notification of these changes to third parties to whom the data were disclosed.

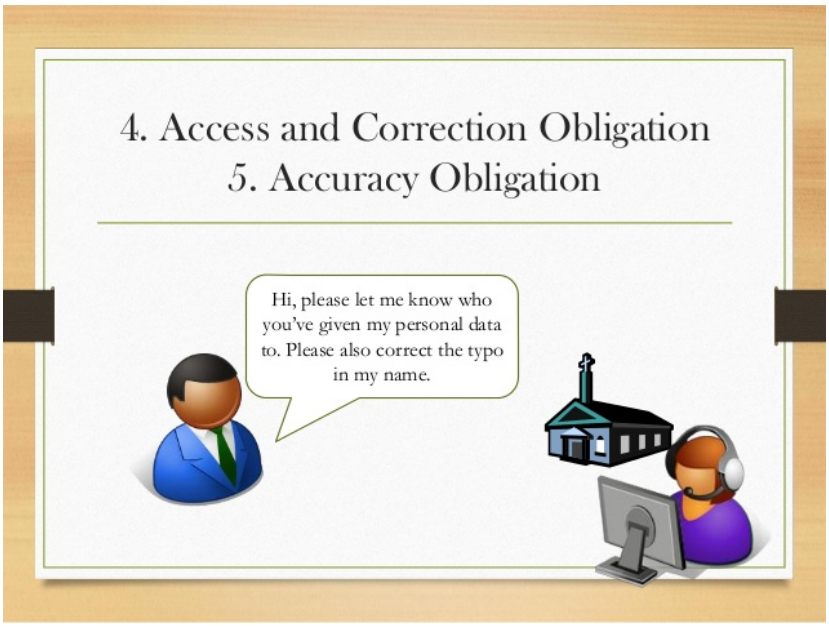


Figure 14: Communication of personal data

- *exemptions and restrictions*: the scope of the principles relating to data quality, information to be provided to the person concerned, the right of access and the publicising of the treatment may be limited in order to safeguard aspects such as national security, the defence, public safety, prosecution of criminal offenses, an important economic or financial interest of a Member State or the European Union or the protection of the person concerned;
- *the right to object to the processing of data*: the person concerned shall have the right to oppose, for legitimate reasons, the processing of personal data and should also have the right, on request and free of charge, to be informed before personal data are disclosed to third parties for direct marketing purposes, and be expressly offered the right to object to such communications (Figure 15);

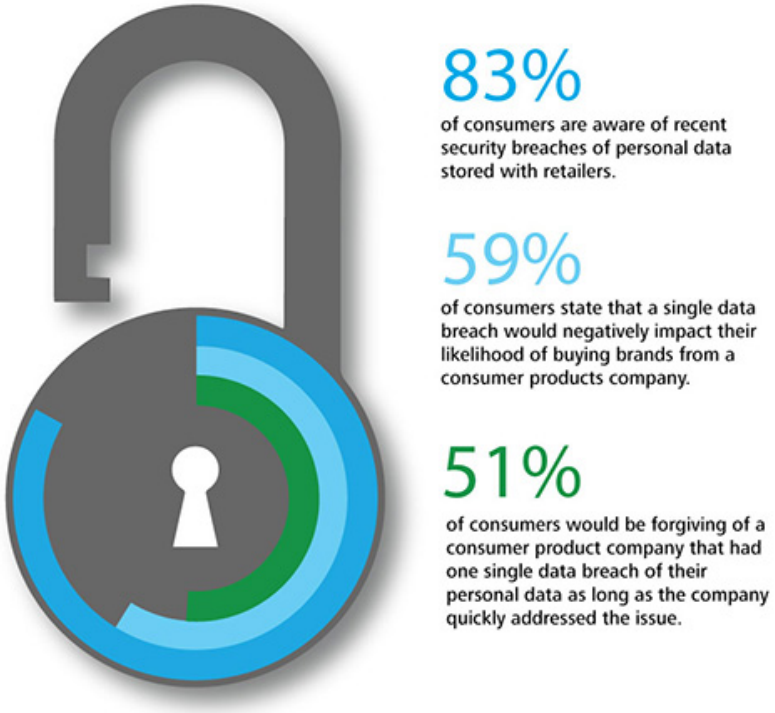


Figure 15: Consumers and personal data

- *the confidentiality and security of processing*: any person acting under the authority of the controller or the executor, including the performer himself, who has access to personal information must treat them only on instructions of the controller. Moreover, the controller must implement appropriate measures to protect personal data against accidental or unlawful destruction, accidental loss, alteration, unauthorized disclosure or access;
- *notification of processing to a supervisory authority*: the controller must notify the national supervisory authority before carrying out any treatment. Prior checks to determine specific risks to the rights and freedoms of data subjects must be performed by the supervisory authority following receipt of the notification. Measures must be taken to ensure communication of the treatments. Supervisors must keep a register of the notifications.

3.7. PRIVATE LIFE

Operators of Web sites often collect information about users through registration pages, and online payments etc. This information is often provided to third parties without giving the user the opportunity to have a control over their use. It is then easy to see how these steps can lead the violation of the privacy of the data.

Facebook is the most representative Social Network. Facebook success is due to the ease of use together with the free service and the impressive number of involved people. The use of Facebook involves many risks to the privacy of the user. Just when you sign up to Facebook, automatically and without the consent of the user, the name of the latter is indexed on search engines outside the network. The data and the user image are then exposed and visible to any third party, even if not subscribed to the community. To unsubscribe from Facebook, the user is not put in a position to easily terminate the service. In addition, all information, images and data are not immediately removed but remains on the server for an indeterminate period, providing a possible reconsideration from the user, contrary to his requirements.

The Privacy Code is easily duped by the various systems by which, within the network, they make sales, steps and data exchanges in total freedom and without put an effective legislative brake on the constant expansion of a real illegal trade on line data.

The right to privacy is the protection of situations and personal affairs by curiosity and public knowledge. Only an experienced person may decide to advertise who has the right to defend from any interference, even if conducted by fair means and not involving harm the honour or reputation or decorum and that the disclosure is not justified for the public interest. The primary source of this right, in Italy, even if it is provided in other more specific rules, is article nr. 2 of the Italian Constitution which states that "*The Republic recognizes and guarantees the inviolable rights of man, as an individual and as social groups in which he expresses his personality*". The violation of this article gives rise to a tort whose injurious effects have to be compensated. The protection of the right to privacy can be requested to the court both by the well-known and not famous person. In Italy, well-known person can enforce his right to privacy exploiting the art. nr. 97 of the Italian Law on Copyright "*Do not need the consent of the person portrayed when the reproduction of it is justified by the reputation or public office, by necessity of justice or police, or for scientific, educational or cultural reasons, or when reproduction is associated with facts, events ceremonies of public interest or held in public. The portrait cannot be exposed, when its display or commercial distribution would prejudice the honour, reputation or dignity of the person portrayed*". This means that the publication of the photograph of the well-known person can take place legitimately even without the consent of the subject, for a public need of information. In fact, the public need of information is constitutionally protected and is always a priority. In case of violation of privacy rights, of prejudice, of moral or asset of a person, the caused damage by this infringement must be proved according to the ordinary rules. In fact, the subject requesting the compensation for the damage caused by that

infringement must prove the verified prejudice to his capital and personnel sphere and the entity and the difficulty to live in that situation.

3.8. THE RIGHT TO DIGNITY

Older people are the most vulnerable regarding privacy. In fact, sometimes, they need to rely on others to perform certain actions and / or to be assisted. This dependence, in many cases, can affect the behaviour of the elderly who, at times, may be contrary to his expectations. In this way, the dignity of the elderly can suffer a limitation.

Dignity is the respect to which every person is entitled to his own nature. Its violation may occur in relation to the seniority and/or disability condition, private life, family life, children, religion, private property, economic initiative, etc.

The idea of human dignity is the cornerstone of the EU constitutional architecture. The article nr.1 of the European Charter of Fundamental Rights says: "*Human dignity is inviolable. It must be respected and protected*". The elderlies and the disabled are the most vulnerable, because sometimes their ability to perform certain actions or the necessity to be assisted, have to depend on other people. Unfortunately, in many cases, it can be easy to induce a behaviour that may be contrary to the expectations of these people, denying or limiting their dignity (Figure 16).

The research on ICT aids and their subsequent experimentation on weak person can sometimes introduce hidden risks that should be considered each time and evaluated and communicated to interested parties.

The European Charter of the rights and responsibilities of older people needed of care and treatment in aging states that if they depend on the support and the care of others, they have the right to make their own life choices and the respect of their free will.

Older people in need of long-term care often see their mobility and self-determination reduced. This may be due to factors that include the obligations imposed on them by those who provide institutional care and/or lack of time of caregivers.

For example, some service providers do not encourage older people to go to the shops to choose their favourite products in person, or not allow people to contribute to the preparation of their own meals for safety reasons.

Some caregivers also cater to older people in overly way without first asking what the elderly wish. It is important to enable elderly people to express their will, opinions and respect their wishes, especially regarding the way they are cared for, their expectations with regard to quality of life and medical therapies.

It is important to understand that the objective of ensuring the safety and security of the elderly is sometimes in conflict with the goal of promoting their autonomy.

Figure 16: The elderly's dignity: The key points

When this occurs, it is important to make a careful evaluation to ensure to achieve a balance between these two aspects and caregivers must recognize that the elderly have the right to run some risks.

3.9. ELDERLY ABUSE

Elderly abuse is defined by the World Health Organization (WHO) as "*a single action, or repeated, or lack of appropriate action, occurring within any relationship where it develops an expectation trust and that causes harm or pain to the elderly person"*. Elderly abuse is often not noticed and is rarely reported. It may be intentional or unintentional, and concerns not only physical abuse, but also psychological and emotional, sexual, financial, pharmaceutical, and negligence. Even the denial of civil rights, discrimination and prejudice because of advanced age are considered forms of elderly abuse (Figure 17, Figure 18).

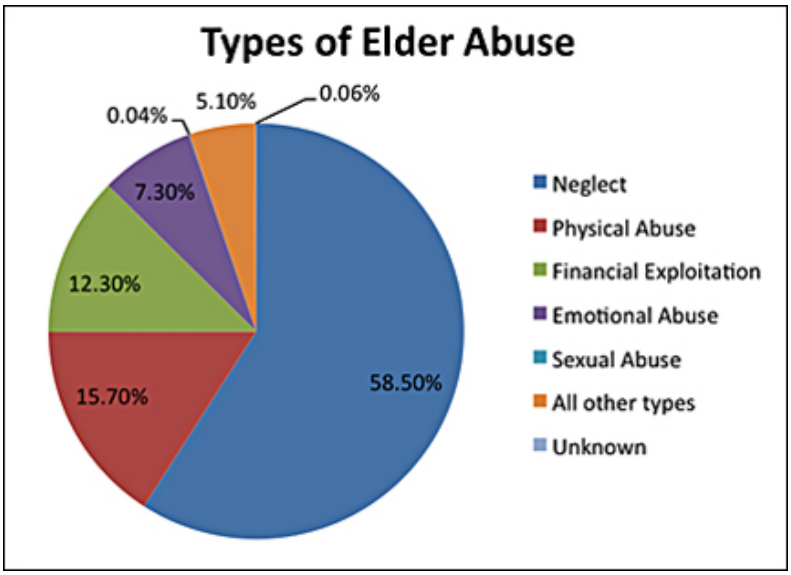


Figure 17: Types of Elder Abuse (National Center on Elder Abuse, Bureau of Justice Statistics. February 16, 2012)

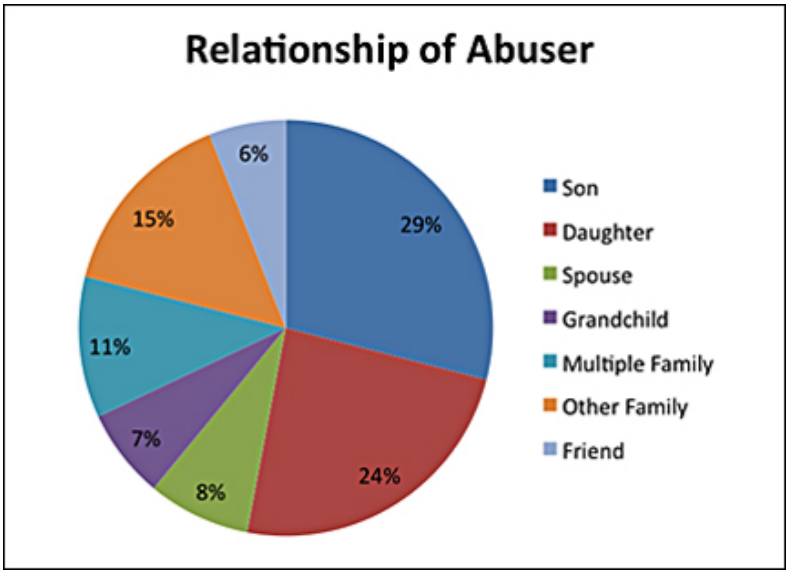


Figure 18: Relationship of Abuser (U.S. Department of Health and Human Services Administration on Aging)

3.10. RISK PREVENTION FOR CAREGIVERS

Despite the huge differences between European Union states regarding the care of elderly, today in many countries the majority of dependent elderly are under the

responsibility of informal workers (e.g. family, friends, neighbours, volunteers) defined caregivers (Figure 19, Figure 20, Figure 21). Informal workers often have high risk of depletion and social exclusion for the physical load and psychological burden. Even professional caregivers are under enormous pressure and do not always receiving training and support that give them a chance to perform in good condition their work. Actions to combat elderly abuse, therefore, must address the needs of caregivers and the difficulties faced by all those - formal and informal caregivers - who devote a significant part of their lives to the frail of elderly, because their needs and the challenges they face are important risk factors. It is duty of public authorities and those who provide care to protect all persons who become dependent on others for their daily needs and allow them to live a dignified life until the end of their existence. Such measures must coexist with measures to protect both the formal and informal caregivers, offering them decent living and working conditions, and recognizing and appreciating the enormous contribution they make to the community.

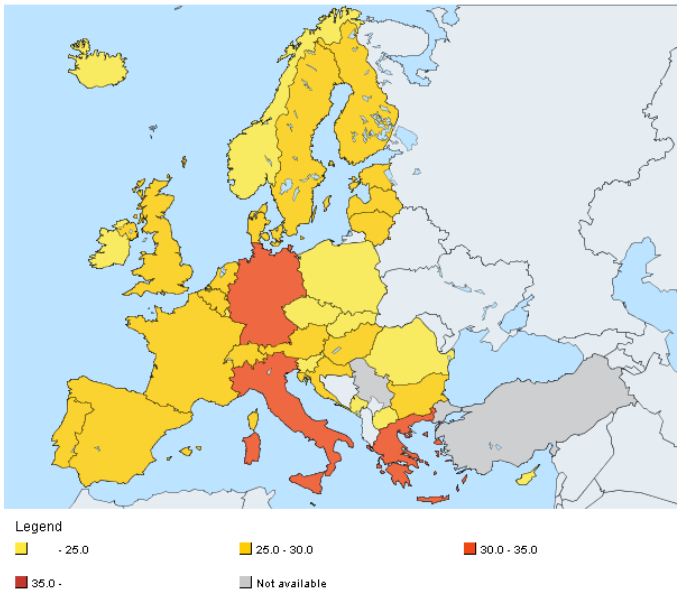


Figure 19: old age dependency ratio (% 2013), Eurostat

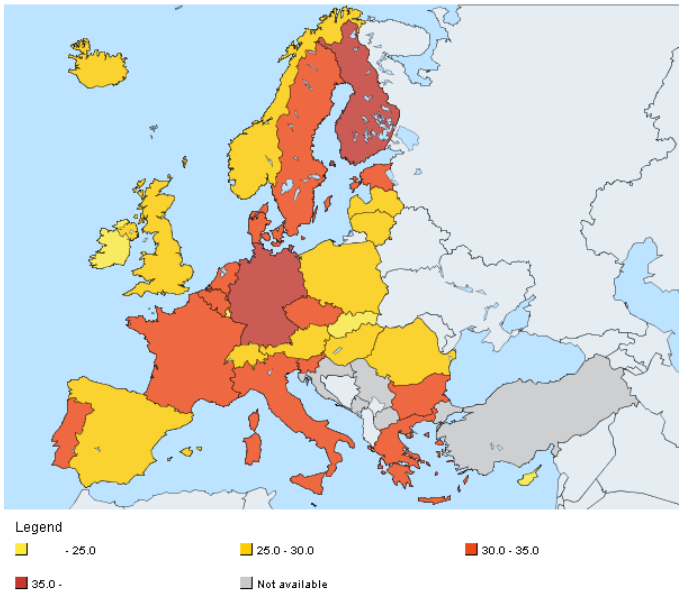


Figure 20: old age dependency ratio (% 2020), Eurostat

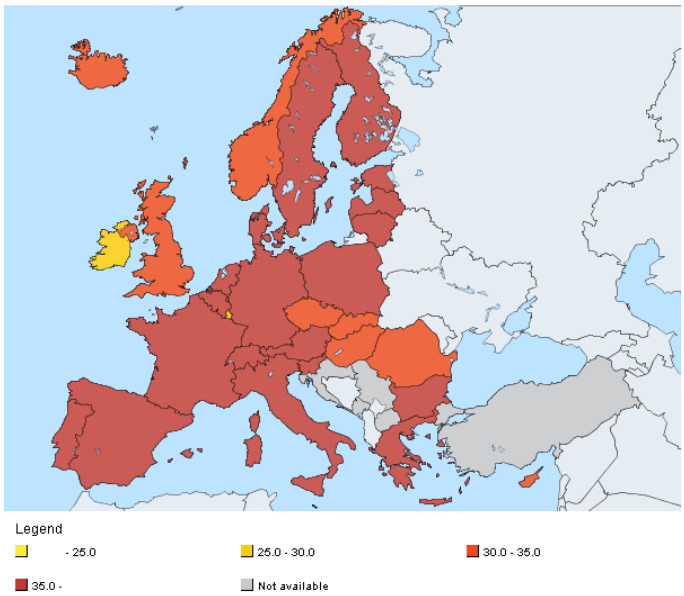


Figure 21: old age dependency ratio (% 2030), Eurostat

3.11. INFINITE PROLONGATION OF LIFE

condition. There are two major scientific theories about technological anti-aging: one is called "compression of morbidity" and the other is called "the indefinite prolongation of life."

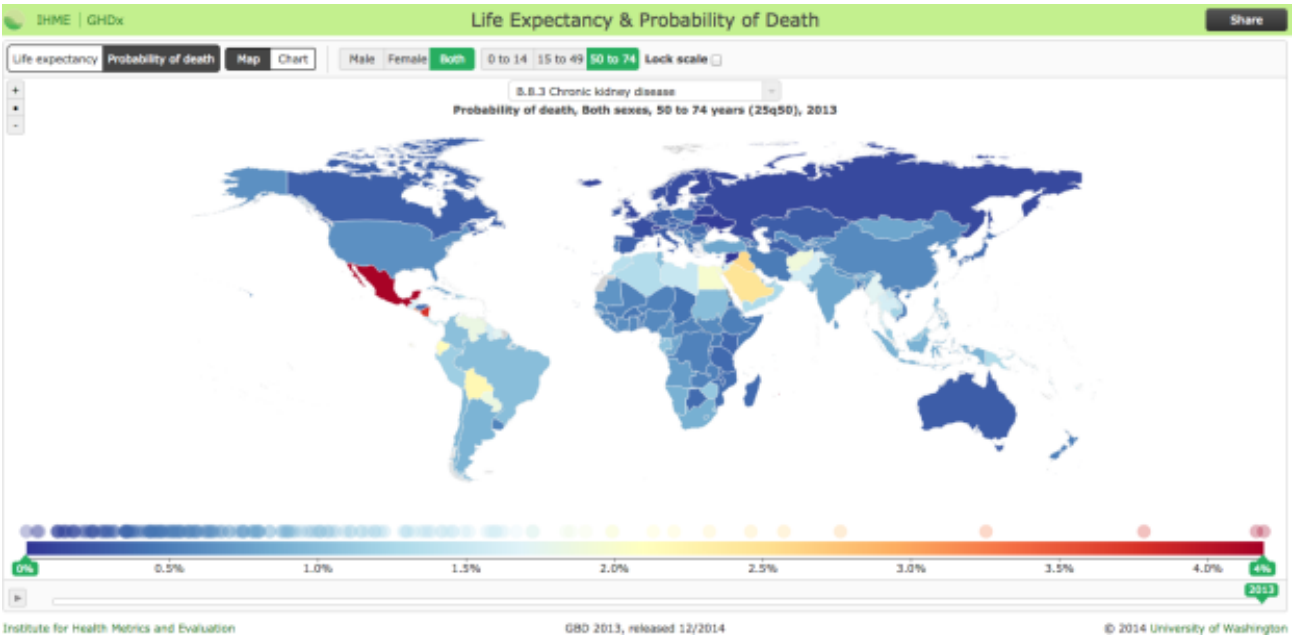


Figure 22: Probability of death among both sexes, ages 50 to 74, 2013

(Global Burden of Disease Study 2013)

The hypothesis state that we are moving towards a society in which all people live in good health up to their genetic limits and then quickly dies in a few days or weeks without becoming an economic burden for society (Figure 22, Figure 23).

Since chronic diseases and disabilities usually occur in old age, the cumulative duration of the disability may be reduced if primary prevention measures will be able to delay the onset of chronic diseases. The decreases in the health risks may also increase the mean age of the death. This means that the hypothesis states that the age of the initial disability can increase and this produces fewer years of handicap and a lower level of cumulative duration of disability. In its extreme view, the hypothesis states that the world is moving towards a society where all people will live in a good health status up to their genetic limits and then they quickly dies in a few days or weeks without becoming an economic burden for society.

The hypothesis of the indefinite prolongation of life is even more optimistic. In this case, it is assumed that genetic limitations can be overcome thanks to the new biotechnologies (for example, cloning, stem cells) and new nano-materials (for

example, nano-prostheses, artificial body parts, enhancers, etc.) and that the boundaries of human life can be pushed further, almost to immortality.

Both hypotheses can generate ethical problems of great complexity and deep meaning. The contemporary techno-science shows an inevitable trend to deny human limitations, senescence and death. Yet it should be clear that there are some issues regarding life and death that technology cannot correct. In his short story "The Immortal" Jorge Luis Borges equals immortality with oppression, irrationality and horror. For Borges, immortality is the absurdity of an infinite repetition without difference, and the immortals are troglodytes unable to speak. Beyond these literary metaphors, assistive technologies for the elderly pose serious questions about our motivations: we are really going to meet the needs of senior citizens, or we use them as an interesting test to evaluate our new powerful technologies?

3.12. THE RIGHT TO INTEGRITY

The right to integrity means that elderly physical and psychological conditions must be respected and no one has the right to violate them without the express permission. This principle is enshrined in numerous international and regional documents. It's also provided for in Article nr. 3 of the Charter of Fundamental Rights of the European Union:

1. Everyone has the right to be respected for his or her physical and mental integrity.
2. In the context of medicine and biology, should be respected in particular:
   a) the free and informed consent of the person in the manner defined by law;
   b) the prohibition of eugenic practices, in particular those aiming at the selection of persons;
   c) the prohibition on making the human body and its parts as such a source of financial gain;
   d) the prohibition of the reproductive cloning of human beings.

This principle should be also applied to the elderly and it is important when considering assistive technologies designed for them. The body of the elderly person is at the centre of different technology strategies. The body of the senior citizen is increasingly technologically modified with implants, pacemakers, artificial sensors, drug dealers, chip under the skin containing medical data and nano-sensors for continuous monitoring of physiological parameters, or for surveillance of older people with dementia etc. There are also important implications associated with monitoring somatic human trials in ICT for the elderly and for informed consent.

3.13. EXCLUSION OF PEOPLE WITH DISABILITIES

The phenomenon of social exclusion of people with disabilities is due to a wide range of social, cultural and political issues that range from those related to the various forms of disability (mental, physical and sensory) cultural and cognitive deficiencies, to environmental phenomena exclusion and difficulties in learning and interrelationship. The EU recognizes and respects the right of persons with disabilities to benefit from measures designed to ensure their independence, their social and occupational integration and participation in community life.

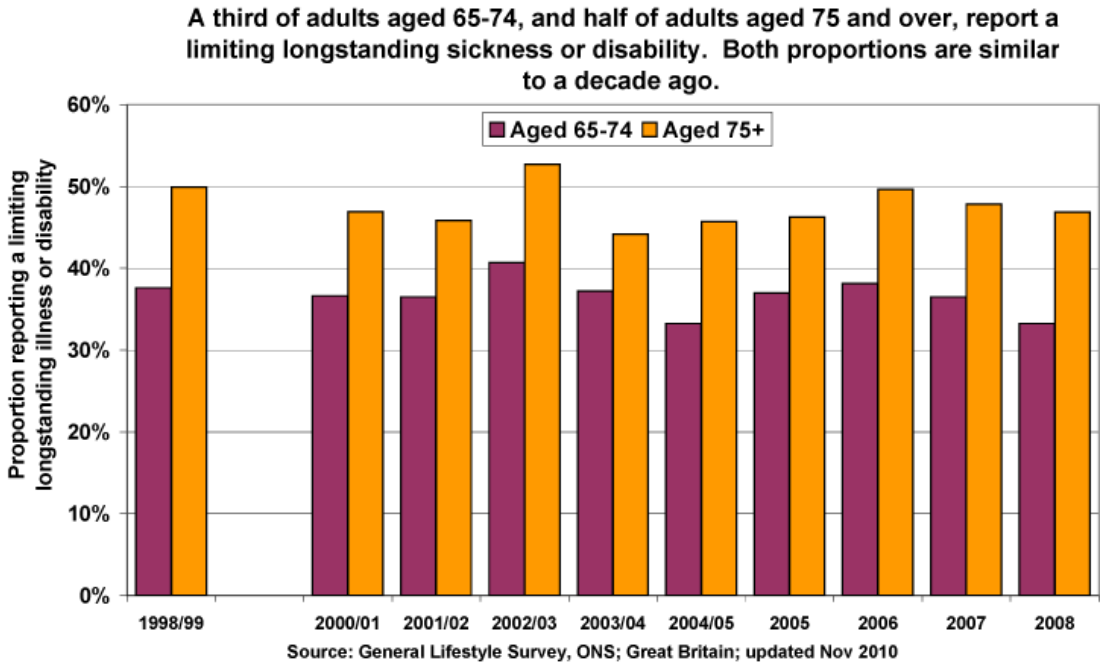


Figure 23: Sickness or disability in adults aged 75 and over.

3.14. THE SOMATIC SURVEILLANCE

The fundamental intuition of M. Foucault (French philosopher, historian of ideas, social theorist, philologist and literary critic) was that "the society exercises control over individuals not only through consciousness or ideology but also in and with the body". This intuition is particularly valid for elderly.

The work of researchers in this field, includes the study of monitoring systems, in which the behaviour patterns of the elderly are monitored and any changes detected are reported. The research analysing the changes in the patterns of behaviour over time to give an early warning of age-related diseases (such as Alzheimer's or Parkinson's) is

already underway. Experts predict that within a decade, a software effective enough to detect the early stages of Parkinson's will be commercially available. Modern technology has also increased the possibilities for monitoring and surveillance of the elderly.

Figure 24: An application to monitor elderly.

Technologies related supervision in the field of care services includes sensors installed on the exit doors, warning about unwanted movement and electronic tags for the localization of the elderly. These technologies have undoubted benefits, but, however, pose serious questions of privacy and ethical issues.

What protocols should be followed when introducing the technology to monitoring? What guidelines must follow an ethic committee to evaluate clinical studies in this field? It's necessary to protect the elderly from abuse by researchers.

Sensitive data produced by ICT services can be a valuable source of information for marketing services for many companies. These systems can be used to discriminate against ethnic groups or other minority groups.

Some technologies are particularly suitable for the generation of particular data (e.g. age, sex, skin colour, etc.), that could be used for the ethnic or religious illegal classification.

Somatic surveillance is a concern in the medical field. Increasingly, consumerist strategies promise eternal youth manipulating the body through bio and nano technologies. As a result, the bodies of older people are invaded by micro sensors and controlled through automatic operations or network commands.

An important principle of privacy is that sensitive data should not be given for essential services, unless the information is essential for the proper performance of such services. This principle is clearly integrated in all relevant EU legislation.

3.15. HUMAN EXPERIMENTATION IN ICT FOR SENIORS

The recent spread of new technologies has contributed to a thinning of the barrier of privacy, such as traceability phones or relative ease to find e-mail addresses of the people for unwanted ads (spam).

Although the geo-location of smart-watch combined, for example, with the inner function of heart rate monitor, can significantly impact on privacy. This system allows marketing companies to track the user in his eating habits and personal tastes through techniques of behavioural advertising, as evidenced by Federprivacy in 2015, and confirmed by a study conducted by the University of Pisa in collaboration with the University Essex and the Harvard Medical School (USA).

It is now ordinary usage that the EU and public and private agencies that fund research require the guarantee that the protocols of privacy are respected in the field of assistive technologies for senior citizens.

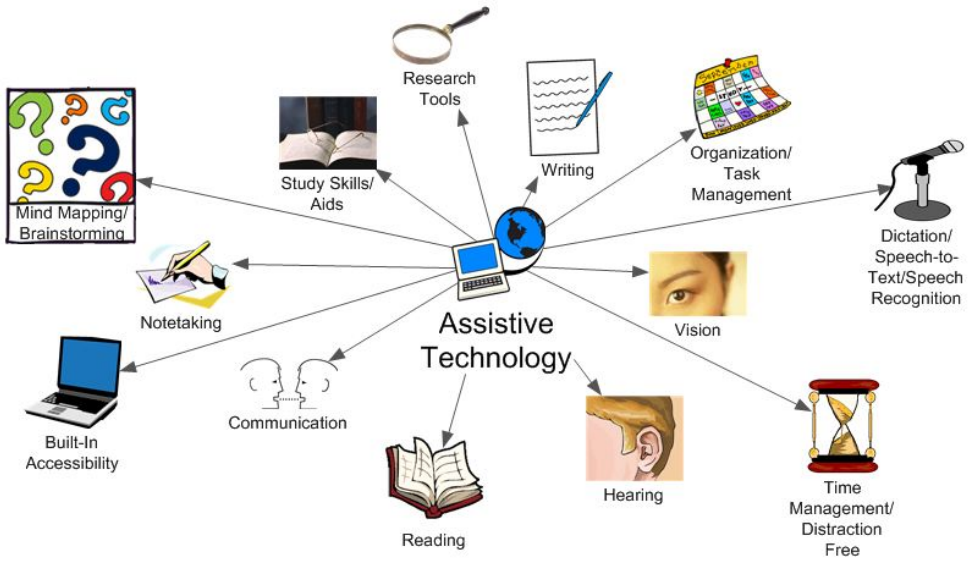


Figure 25: Example of assistive technologies

However, there are some important issues to be addressed, such as the following:

- an elderly person cannot be considered vulnerable by the mere fact of being old. There is no doubt that many seniors suffer from social, mental and physical limitations, and so, of a frag-ile condition. Can be defined specific criteria for assessing the vulnerability of older people participating in ICT research?
- assistive technologies (Figure 25) are often driven by actors who are not doctors, in environ-ments away from traditional medical settings, involving persons who are not medical patients.

This makes very difficult to apply the medical rules to ICT research. For example, are there local ethic committees that verify the correctness of the proposed actions? What could be the "risk" if the research has a direct interest from some organizations or companies?

3.16. THE INFORMED CONSENT

In Italy, the informed consent (Figure 26) is the permission of the patient to receive any medical treatment after the necessary information on the case by the doctor proponent.

The Code of Medical Ethics states the general principle that it is forbidden to the doctor to express diagnosis and/or to undertake treatment without gaining informed consent of the patient. There is the obligation for the doctor to give up the consequent diagnostic or curative, in the presence of documented refusal of the person capable of discernment. It is not allowed any medical treatment against the will of the person. Therefore, today the legitimization of the medical activity can no longer find its basis on the prestige and authority of the doctor, but only and exclusively on the informed consent of the patient.

Figure 26: Example of informed consent module

The patient must be properly informed about the treatment that he will be submitted and the risks that they may derive from such treatment. Information given to the patient is an integral part of the medical service like the medical performance, the diagnosis and the operation.

It is now established the principle that no conscious and capable person of discernment can be subjected to any medical treatment without or against his will.

The purpose of seeking informed consent is therefore to promote the autonomy and freedom of choice in the field of medical decisions.

In the case of elderly patients with severe cognitive problems that can rise to an inability to make decisions, the doctor, after an interview with the family of the patient, may appeal to the judicial authority to request an administrative support or other safety to protect the patient.

Some elderly live independently in their own homes and others require attention and care by a third party, family members and / or professional caregivers. The latter category of seniors can be divided between those who need care and live in their own homes and those, however, who need assistance in a nursing home.

Regarding the use of new technologies for the elderly or people with disabilities and with special social needs, there is the need of specific guidelines.

Seniors who are able to understand the benefits of new technologies, should be informed on how could or should be used technologies and if there are potential impacts about privacy or ethical concerns. Many seniors are certainly willing to give up a potential loss of privacy in exchange for added security and protection, however, they must be informed explicitly, not only for the benefits but also for the risks and what measures will be taken to minimize these risks.

Service providers that implement these technologies, for example in the projects, could find very useful to have the elderly participants to be interviewed explaining why the use of the technology, the benefits and perceived risks and prevention measures. For example, how their data will be protected, who will have access to such data, images or video or audio recordings, for how long to retain the data, as they could be treated, and so on. Although a consent form is signed, this should not exempt the service provider's responsibility to clarify the use of the technologies.

In some cases the initiative of the use of new technologies, products or services, is taken directly from the elderly person who however must be kept informed by the service providers and/or producers.

This obligation is as that imposed on pharmaceutical companies that need to provide information not only about the disease to be treated using their product, but also about possible side effects and what to do in case one or more of these contraindications arises.

It should also be considered, not only in the case of older people but in general, the language used for information between suppliers and consumers. There is a risk that the consent may not be really informed or that the consumer gives his consent reluctantly if he want to use in any case the product or service. In this case he will have to accept the terms and conditions even if he does not agree with that. In many cases, the information provided may be too complex or difficult to understand, the privacy policies of many suppliers are abstruse or ambiguous and therefore consumers may not be willing to spend time trying to decipher the information provided.

Informed consent in the case of a consumer that suffers of a disability, such as visual, hearing and physical impairment, technologies and/or services must be designed taking into account such considerations.

An ethical issue is when the elderly person is able to understand the benefits and risks of technologies and however, he choose to don't use a particular technology, even when the professionals believe that he should do it.

Consider for example elderly people with personality disorders for which, although he has not committed, knowingly or unknowingly, any fault or damage, social workers believe that should be useful having the elderly tracked or monitored because he represent a potential risk for himself or for the others.

Policy-makers, designers and suppliers of technology must consider the mechanisms by which it can be assured that the consumer has really been informed. So to make sure that the consumer is consenting, free and able to choose the service, without any negative repercussions.

The issue of informed consent regarding the use of technology and the elderly or persons with disabilities is not simple.

Ethical guidelines and measures should have appropriate regulation, where informed consent is mandatory and desirable.

3.17. LONELINESS AND SOCIAL ISOLATION

The word loneliness includes at least two different concepts: loneliness and isolation. These are concepts that are often confused. There are important differences between being emotionally isolated and be socially isolated.

Loneliness is the subjective perception of being deprived of relationships and social contact with other people, to be excluded from the community, to feel alone when instead not wanting to be. Loneliness is a psychological state. Loneliness reflects a dissatisfaction in social relations, can arouse feelings of aggression, which in turn inhibit the ability of the person to acquire and develop supportive relationships rebuilding his personal network. In other words, sooner or later, loneliness leads also to isolation.

Isolation is the objective condition of having too few or poor social ties and the concrete condition of living alone (Figure 27).

Both the loneliness and the isolation can be perceived in a positive way. People may want to be emotionally or socially alone to attend to the values that are deemed to be more important than social ties.

The idea of solitude as a positive condition is implicit in the notion of emotional or social independence. Sometimes this independence suggests an ability to survive or even of wellbeing, in the case where the emotional and social ties are weak or absent. In fact, despite the stereotypes, the elderly tend to find the condition of isolation less

painful than younger people. Some deliberately seek to be alone, as an expression of independence.

However, numerous medical and psychological studies have shown that prolonged emotional or social loneliness is likely to endanger the physical and mental condition of the people.

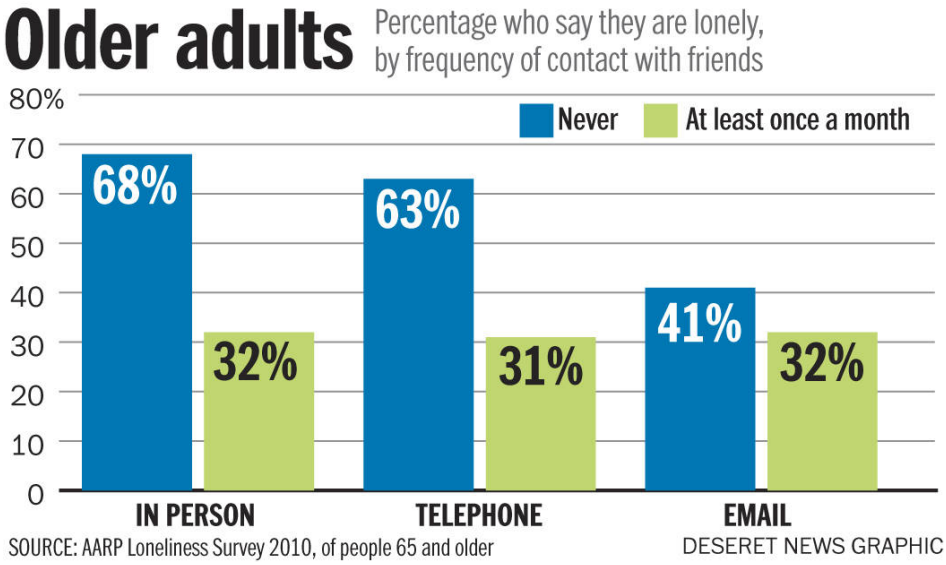


Figure 27: Loneliness and frequency of contacts with friends

Researchers have shown that isolation and loneliness tend to accelerate the rate of physiological decline due to age. New technologies are therefore careful to isolation and loneliness.

Today we see a real decline in birth rates, the family is getting smaller and mobility increases the physical distance between generations of a family, thus increasing social isolation. So the new forms of communication, smartphones, e-mail, messaging, web meetings and social networking, are useful to alleviate this isolation.

However, not all older people will make full use of the new communication tools made available to the scientific community and these instruments are not able to overcome the isolation due to digital illiteracy. Furthermore another critical factor is due to the digital divide. The gap, however, is set to decrease in the coming years.

To meet the specific needs of elderly, specific tailored web sites was realized for them.

In the near future virtual friends will play an important role in the lives of senior citizens. Robotic pets for seniors are already a reality and are very useful for the elderly with dementia. Some scientists believe that robots are the answer to caring for an aging population, robot-like puppies with integrated sensors allowing elderlies to respond, e.g.

with the movement, with the contact and with the voice. At the same time, these robots can be used to monitor the safety of the elderlies via remote access.

Some fellow robots are already in use, e.g. the dog AIBO (Artificial Intelligence roBOt) is one of the robotic animals developed by Sony, since 1999, in various models. It is able to perceive sounds and noises, see and move autonomously. The robot detects the surrounding environment (SIFT algorithm) using a tiny camera, it recognizes voice commands and evolve from puppy to adult animal.

The new technologies of communication and robot companions, however, raise some concerns, regarding privacy concerns and objections about the goodness of virtual contacts compared to human ones.

Another aspect to consider is that the new communication technologies can decrease the interest in going outside the home, this would only exacerbate the reduction of direct face to face contact.

However, the consideration that the digital world and the robots are the elderly social life can become humiliating and damaging the respect of the person.

Aging and life expectancy of European society is increasing. Emerging areas are: social technologies, robots, virtual friends for the elderly, anti-aging technologies and surveillance technologies.

An ethics of digitization that protects individuals from illegal intrusion, which is based on the right to privacy, the right to data protection and to informed consent of the person, does not meet the social and privacy needs in ICT for the elderly. It is therefore necessary an ethic flexible and dynamic solution to allow individuals with different skills to forge and remain active in society expressing and sharing their opinions.

3.18. THE SOCIALIZE SAFEGUARD

The principles and underlying assumptions outlined in this document, will be taken into account and applied within Socialize services, creating, in this way, a proper Socialize Safeguard.

In detail, taking into account the services that will be put in place and that are described in deliverable D1.7 (Use cases), it is expected that:

1. The data will be managed only by authorized personnel, including maintenance and administration operations on the platform system. They will be treated on the basis of fairness, legality and transparency principles, and principles relating to the protection of confidentiality and of the rights of subjects entitled to such rights.

   Data treatment will be performed through data processing and storage modes so that data and communication confidentiality are ensured in accordance with current regulations.

2. The right to participate will be put in place through the services that facilitate e-participation that will be the Socialize Forum and the Socialize Social Network. The implementation of their capabilities will allow that personal information will be:
   - fairly and lawfully processed;
   - processed just for the Socialize project purposes;
   - only those necessary to the effectiveness of the system purposes;
   - accurate and up to date;
   - kept for duration on the project only;
   - processed in line with the data suibject's rights;
   - secure;
   - not be trasferred to other places.

3. The individual will be enable to control access to information about him or herself through the "User and Billing" Socialize service.

4. The individual will be enable to develop his own personality within a network of other human individuals using easily the whole Socialize platform, primarily made specifically for this purpose. Socialize will create also favourable conditions to guarantee the right to establish and develop relationships with other human beings.

5. Specifically the Socialize Forum, the Socialize Social Network, the Time Bank, the Photo Book and the Social Gaming services, will permit to the elderly to avoid loneliness and isolation and he will have a real access to other people and networks of people.

6. The data will be only processed if the subject has given consent signing an informed consent module.

7. Will be provide to the subject from whom data are collected (the identity of the controller, the purposes of the processing, recipients of the data, etc.).

8. The system doesn't collect information about users through registration pages, and online payments, etc. If a user unsubscribe from any Socialize service, all information, images and data will be immediately removed.

9. The Socialize Forum and the Socialize Social Network services, will enable elderly people to express their will, opinions and respect their wishes, especially regarding the way they are cared for, their expectations with regard to quality of life and medical therapies.

10. The Monitoring Data Analisys service will be implemented making a careful evaluation to ensure to achieve a balance between the objective of ensuring the safety and security of the elderly and the goal of promoting the elderly autonomy.

11. The Social Forum and the other services permitting social interactions, will implement special functionalities offering to caregivers effective working conditions to customize and adapt these services to the real elderly needs.

12. The Remote Support, the Communication System and the Easy Access HMI services will help to avoid the social exclusion of elderly people with disabilities, allowing easy access to the system and providing tools to a remote help the user from appropriate specialized professional figures. These instruments will be built ensuring a possible access to the user's PC protected by password and explicit user consent.

13. Because many seniors suffer from social, mental and physical limitations, and so, of a fragile condition, elderly will be protected from abuse by researchers accordingly with the guidelines shown in the D1.1 deliverable.

14. Service providers Socialize Project parteners will explain to the elderly users why the use of the technology, the benefits, how their data will be protected, who will have access to such data, images or video or audio recordings, for how long to retain the data, as they could be treated, and so on.

15. To avoid that the new communication technologies could decrease the interest in going outside the home exacerbating the reduction of direct human contact. To try to reduce this risk, the Social Forum service will include the ability to display on a geo-localized map the real places of discussed events, as well as to facilitate the ability of people to meet face to face each other.

3.19. BIBLIOGRAPHY

- 1890 -The Right to Privacy - Warren e Brandeis - Harvard Law Review. Vol. IV - December 15, 1890 - No. 5
- 1948 - The Universal Declaration of Human Rights
- 1948 ONU - Dichiarazione Universale dei Diritti Umani - Il 10 dicembre 1948, Assemblea Generale delle Nazioni Unite
- 1950 Roma - Convention for the Protection of Human Rights and Fundamental Freedoms - Rome, 4.XI.1950
- 1965 - WARNER, S. L. 1965. Randomized response: A survey technique for eliminating evasive answer bias. J.Am. Statistical Assoc. 60, 309, 63–69.
- 1966 - International Covenant on Civil and Political Rights - General Assembly of the United Nations on 19 December 1966
- 1981 - CHAUM, D. 1981. Untraceable electronic mail, return addresses, and digital pseudonyms. Comm. ACM 24, 2, 84–88.
- 1981 - Teoria dell'agire comunicativo - Jurgen Habermas
- 1987 *Il discorso filosofico della modernità. Dodici lezioni*, (trad. di Emilio Agazzi e Elena Agazzi) - Laterza, Bari-Roma 1987 ISBN 88-420-2940-8
- 1989 - Habermas, J. (1989). The structural transformation of the public sphere: Inquiry into a category of Bourgeois society. Cambridge, MA: MIT Press.
- 2001 - European Commission. (2001) European Governance: A white paper, COM(2001) 428 final, Brussels, 25 July 2001.
- 2001 -Soderman, J. (2001). Transparency as a fundamental principle of the European union. European Ombudsman. http://www.euroombudsman.eu.int/speeches/en/2001-06-19.htm
- 2002 - The Toronto Declaration the Toronto Declaration on The Global Prevention of Elder Abuse - 17 November 2002
- 2004 - Ethical Guidelines for undertaking ICT research in FP7 - ftp://ftp.cordis.europa.eu/pub/fp7/docs/guidelines-annex5ict.pdf
- 2005 -JIANG,W. and CLIFTON, C. 2005. Privacy-preserving distributed k-anonymity. In Proceedings of the 19th Annual IFIP WG 11.3 Working Conference on Data and Applications Security. 166–177.
- 2006 - EMAM, K. E. 2006. Data anonymization practices in clinical research: A descriptive study. Tech. rep. Access to Information and Privacy Division of Health in Canada.
- 2006 - GEHRKE, J. 2006. Models and methods for privacy-preserving data publishing and analysis. Tutorial at the 12th ACM SIGKDD.
- 2006 - Riga Declaration - 11-13 Giugno 2006

- 2007 - CARLISLE, D.M.,RODRIAN, M.L., AND DIAMOND, C. L. 2007. California inpatient data reporting manual, medical information reporting for California (5th Ed), Tech. rep., Office of Statewide Health Planning and Development.
- 2007 - *European i2010 initiative on e-Inclusion* - To be part of the information society
- 2007 - European Commission. (2007). The European research area: New perspectives. Green paper. COM(2007) 161 final. Brussels, .4.4.2007.