

# Cameras in your living room, the next step in e-homecare?

## Executive Summary

Although the positive effect from the use of cameras in eHomecare on patients has been demonstrated, it also makes care more privacy intrusive: capturing us on film in our most personal, most intimate environment, our own home. This paper examines the protection of the patient, on the one hand, and occasionally filmed persons, on the other, when using video monitoring systems in eHomecare. Three protective mechanisms will be discussed in this specific setting: the right to protection of personal data, the right to privacy and the right to personal portrayal.

First, images and sounds from a patient made with an observation camera are protected by the Data Protection Directive. There is, however, discussion going on with regard to the protection of occasional visitors. Discussion also arises with regard to the protection of the processed data as sensitive data. The patient's data are likely to be qualified as health data, and thus protected more stringent. Data of occasional visitors are, in contrast, most likely not to be thus qualified. Secondly, the patients themselves will undoubtedly also be protected under the broader right to privacy, but occasional visitors risk to fall by the wayside. Last but not least, the images will also be protected by the right to personal portrayal when the captured persons are recognizable.

Due to these three protection mechanisms, the use of cameras as a next step in eHomecare will currently have to be based on the consent of the patient. Whether or not occasional visitors need to be warned about the use of cameras is, however still open for discussion.



Griet  
Verhenneman

Legal Researcher  
ICT

ICRI - K.U.Leuven - IBBT

## Keywords

Cameras, health data, privacy, data protection, portrait rights

“ When cameras are placed in people's homes, the images made can be protected by three different legal mechanisms: the protection of personal data, the protection of the right to privacy, and the protection of the right to personal portrayal. ”

## 1 Introduction

Our society, including our health- and homecare, is more and more confronted with visualization. In hospitals we use high definition x-rays, 3D scanning and observation cameras. In homecare, it has been announced that the use of digital imaging, interactive webcams and even camera-nursing will be soon introduced. There are many benefits brought by this increased use of visualization. However, it also makes care more privacy intrusive. Operating cameras in and around homes is often seen as one of the most privacy intrusive practices, since it captures us on film in our most personal, most intimate environment.

The Belgian IBBT project TranseCare<sup>1</sup> is currently developing a video monitoring system, as part of an ICT platform, which can assist people under care and their family and health professionals. The overall objective of the TranseCare platform is to support people suffering from a chronic disease and/or from degenerative disabilities due to age through the aid of an ICT platform. The TranseCare project wants to take the concept of “independent living systems” a step further by among the use of other components, the use of a video monitoring system. Already in the early stages of the project, the consortium came up with two different kinds of systems that could be used. We could opt for a system with cameras that can only be switched on in emergency situations, or a system, which monitors continuously. Within the project, the consortium decided not to develop continuous monitoring. This choice was made, not so much for technological or legal reasons, but mostly with the social acceptance in mind. Legally, specific questions with regard to privacy and the protection of personal data arise in both cases.

This paper will elaborate on the protection of personal data, the right to respect privacy, and the right of personal portrayal, currently being the main legal mechanisms, which protect our privacy, when cameras are installed in our homes.

## 2 Data protection

In Europe, personal data are protected by the Data Protection Directive 95/46EC (hereafter DPD), which has now been implemented by the member states. In Belgium, the implementation of the directive resulted in an adjustment of the Data Protection Act of December, 8, 1992 (hereafter DPA). This paper will however be restricted to the discussion of the DPD, and thus European Law, as much as possible.

As always, the first main question to be asked is whether the DPD is actually applicable to the use of cameras in peoples' homes. Data protection laws are only applicable when “processing” of “personal data” takes place. So to answer to this question, the first issue to explore is the interpretation of those essential terms used by the DPD. It has to be verified whether or not “personal data” are being “processed,” when using a video monitoring system in a homecare setting.

In a second stage, a distinction will have to be made between the protection of “normal” personal data and “sensitive” personal data, including health data. It will be examined whether or not the personal data captured by the video monitoring system are protected under the stricter regime of sensitive data.

---

<sup>1</sup> “Transparent ICT platforms for eCare” is a Belgian project supported by the Flemish Institute for BroadBand Technologies (IBBT). IBBT is an independent research institute that stimulated innovation in ICT by order of the Flemish government. IBBT brings different partners, from the industry, universities, non-profit organizations and governments together in multidisciplinary research projects, such as TranseCare. More information on the project and the partners involved can be found on the following website: <http://project.ibbt.be/transecare>.

In both stages a further distinction will also have to be made between the protection of the patient and the protection of occasionally or incidentally filmed persons.

## 2.1 Essential terms in the DPD: “processing” and “personal data”

As indicated above, the Data Protection Directive is applicable to the “processing” of “personal data”.

The term “processing”, according to the Directive, means “any operation or set of operations which is performed on personal data whether or not by automatic means such as collection, recording, organization, storage, adaptation or alternation, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction” (article 2, (b) DPD). This includes any form of handling of personal data, regardless of whether automated processing is involved or not, and from the very first stage of its collection. Given the Directive has opted for a broad definition, reinforced by an extensive interpretation by the Article 29 Working Party<sup>2</sup>, capturing images with a camera, whether these images are stored or not, clearly has to be regarded as some kind of data processing.

Next, the DPD defines “personal data” as “any information relating to an identified or identifiable natural person, the data subject” (article 2, (a) DPD). Given, again, the very broad definition, both on the European level and, at least in the case of Belgium, on the national level, it is acknowledged that images, just like texts, sounds and even radiofrequencies, can be are personal data, at least whenever they refer to identifiable individuals<sup>3</sup>.

The DPD does not define when an individual is identified, but since it allows for identifiability, it does not require the last and highest degree of identification, that is, unique identification as for instance by a DNA profile. An individual can also be identifiable when he can be identified, directly or indirectly, by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity. To determine whether level of information is high enough to be qualified identifiable, account should be taken of all the means likely reasonable to be used to identify the said person (Recital 26, Bullesbach et al., 2006). This will have to be assessed case-by-case according to a proportionality criterion. It follows that what is of legal importance is the capability or potentiality of identification rather than the actual achievement of identification. However, whenever the process of identification requires the controller to deploy disproportionate efforts, data will not qualify as “personal” (Coudert & Dumortier, 2008; Bygrave, 2002).

## 2.2 Applicability of the DPD to the use of a video monitoring system

Though the DPD thus has a very broad scope, discussion arises when applying the definitions of “personal data” and “processing” to the use of a video monitoring system and more specific with regard to the images and sounds captured by this system. This is not so much the case with regard to specific patients, but certainly is with regard to incidentally filmed persons, like the patient’s wife or husband, visitors or the cleaning lady.

<sup>2</sup> See for instance, Article 29 Data Protection Working Party, Opinion n° 4/2007 on the concept of personal data, WP 136, 20 June 2007.

<sup>3</sup> At the European level, this was acknowledged by the Article 29 Working Party in its opinion 4/2004 on the processing of personal data by the means of video surveillance of 11 February 2004, 5 and in Recital 14 of the DPD. In Belgium, this was acknowledged by the Belgian Privacy Commission in both its advice nr. 14 of 7 June 1995 and advice nr. 34 of 13 December 1999.

With regard to the patient who is being observed by the video monitoring system, whether this is a continuous monitoring or not, the applicability of the DPD is clear and generally agreed upon. The camera processes - captures on tape - personal data - the image of the patient. The patient is easily identifiable on the images and the images are made with the intention to identify the patient and his health situation. With regard to occasionally or incidentally filmed persons however, there is no unanimous stand<sup>4</sup>.

#### Applicability of the DPD to images of occasionally or incidentally filmed persons

Some, like the Belgian Privacy Commission, are convinced that images of natural persons cannot be qualified personal data when made accidentally or incidentally<sup>5</sup>. This is because they argue that the purpose for making the images is decisive.

Others, however, do not take the purpose of the processing as a starting point, but rather evaluate the images according to their identifiability. They argue personal data are being processed every time a person is filmed, accidentally or not, at least when this person can be identified without unreasonable means or effort.

Although no explicit statement on the issue has been made, the Article 29 Working Party tended to agree with this second opinion. In its latest opinions, however, the Working Party seems to be mainly aiming for a flexible and usable interpretation of the DPD, and therefore now considers the purpose of the processing as a possible criterion. The Working Party interprets “data relating to a natural person” as data concerning that person. Therefore, one could argue that images of identifiable persons, accidentally made, are not personal data, since these images are not used to evaluate or influence the filmed person, and thus does not concern these persons<sup>6</sup>. Two examples can be given to clarify the differences between both opinions.

The first illustration is what has been called the “pond and ducks example”. A camera is set up in a park to observe ducks on the pond, but passersby are also captured on tape. According to the first opinion, the images of the passersby do not have to be considered as personal data, since the purpose of the filming was the observation of the ducks and not of people walking nearby. According to the second opinion, however, these images are personal data when the passersby are identified, or identifiable without unreasonable means or effort.

The second illustration concerns the monitoring of a barrier in a car park. The barrier is filmed not to observe the people in the cars, but to make sure cars can easily get in and out. According to the first opinion, no personal data are being processed even though people are being filmed, since the purpose of the monitoring is only to ensure smooth traffic flows. According to the second opinion, however, personal data are being processed simply and solely because the faces of the people in the cars are filmed as well. This, of course, unless the tape is so unclear that people cannot be identified without unreasonable means or effort. The second opinion only takes the purpose of the processing into account at a later stage, when assessing the lawfulness of the data processing.

Coming back to the use of cameras in a living room of a patient, the discussion is the same. When

<sup>4</sup> For the sake of completeness it has to be added that this discussion does not only rise in healthcare scenarios, but for instance also with regard to surveillance cameras. See Bullesbach, Pouillet and Prins, *Consisse European IT Law*, Kluwer Law International, The Netherlands, 2006, 32.

<sup>5</sup> *Advice Belgian Commission for the Protection of the Privacy*, June 7th 1995, n° 14, 2; *Advice Belgian Commission for the Protection of the Privacy*, December 19th 1999, n° 34, 2.

<sup>6</sup> *Opinion 4/2007 Article 29 Data protection working party*, June, 20<sup>th</sup> 2007, <http://www.ec.europa.eu/justice-home/fsj/privacy/index-en.htm>, 10.

using a camera to observe a patient, the first opinion implies only personal data of the patient are being processed (and therefore protected by the DPD), and not the images of occasionally filmed persons. The second opinion on the other hand, implies that not only the images of the patient will be protected, but also those of these other persons. This is, again, at least when these other persons are identified or identifiable, which is exactly what the discussion will then be all about.

Both opinions make valid points, which means that it will eventually be up to the sovereignty of the judge to make a choice between the two. Next to that, I am convinced that the choice will not be purely legal, but will also be influenced by business strategies. I would, however, want to stress that the consequences of the choice are extensive, as this decision implies the choice for the protection, or hardly any protection, of accidentally filmed persons. However, as it will be elaborated below, this is not the end of the story as there are two other protection mechanisms apart from the DPD.

#### Applicability of the DPD to sounds

The Council of Europe has explicitly recognized that sounds can be qualified as personal data, at least under the always present condition of identifiability<sup>7</sup>. This is also acknowledged in article 33 of the DPD.

With regard to the use of cameras in people's homes, this implies that also recorded sounds may be qualified as personal data. Furthermore, when images and sounds are captured together, the level of identifiability rises. However, with regard to sounds captured from occasional visitors, the same discussion as described above will arise.

### 2.3 Protection of health data and the use of a video monitoring system

The DPD makes a distinction between "normal" personal data and "special categories" of personal data. At the European level (unlike on the Belgian level), these special categories are mentioned, but not defined. One of those categories is the data concerning health data. In the recommendation of the Council attached to the DPD, it is stated that data concerning health require "a strong and clear link" to the health of the person<sup>8</sup>. The European Court of Justice, however, held in the Bodil Lindqvist case that "the expression 'data concerning health' [...] must be given a wide interpretation so as to include information concerning all aspects, both physical and mental, of the health of an individual" (Bullesbach et al., 2006).

In Belgium, health data are defined as "data concerning health", which implies that the health (or a health condition) must be directly shown. This seems a bit stronger than the interpretation of the Council and the ECJ<sup>9</sup>.

However, the essence of the definition is often illustrated with a picture of a man in a wheelchair at a park. In the picture, you can clearly see the man is handicapped, but the picture was not taken for the sake of the handicap or health of the person, so the picture itself does not have a direct connection to the man's health. Whereas, when the same person is photographed, e.g., at a disability examination and this picture is added to his health record, the picture does connect directly with the

7 See Opinion 4/2004 Article 29 Data protection working party, February 11th 2004, <http://www.ec.europa.eu/justice-home/fsj/privacy/index-en.htm>, 5; Convention No. 108/1981.

8 R (97) 5 on the Protection of Medical data, European Council, February 13th 1997, <http://www.1.umn.edu/humanarts/instree/coerecr97-5.html>, 2.

9 For the sake of completeness, it has to be stressed that, although there might be a slight difference between the Belgian and European interpretation, due to the member states' freedom, when transposing directives into national law, it must not be forgotten that in the case of lack of clarity one must always take into account the original intention of the directive.

man's health and will be qualified as health data<sup>10</sup>.

When applying this reasoning to the use of cameras in a homecare setting, we are, again, faced with a dilemma. At this stage, however, the dilemma arises with regard to the patients and not so much with regard to the occasional visitors / incidentally filmed persons.

With regard to the monitored patient, it could, be argued images made in the different rooms of the patient's home are not health data because they do not relate directly to the health of the patient. Though information about the patient's health can be derived from the images, the images were primarily not taken for the sake of healthcare, the purpose of the video monitoring system not being continuous or occasional monitoring of the health status of the patient, but rather being support for daily life or allow quick and efficient response in an alarming situation. On the other hand, the camera often will be placed in the home specifically because of the high risk for health problems. In that case, the images will only be viewed for health purposes, and therefore it could also be argued that they are health data. This second interpretation is reinforced when the monitoring system does not monitor the patient at all times, but only when an alarm is activated, indicating a health problem is occurring.

However, it must be stressed the qualification of the images made by the video monitoring system will require a case-by-case approach and evaluation, much depending on the purposes of the video monitoring system.

As already announced, this reasoning also needs to be evaluated with regard to occasionally filmed persons. As indicated above, it is plausible to argue that personal data are being processed when persons are occasionally filmed by a video monitoring system. However, considering the images of occasional visitors as possible health data is, at least in my opinion, a step too far. It is possible that the existence of a health condition can be established from the image, for instance that a person has a broken arm. However, the image will never refer directly to the health of this person and even more important, there should be no intention what however to monitor their health via the camera.

### 3 Protection of the right to privacy

The protection of personal data is only one part of the protection of the right to privacy. Since, as described above, some argue that occasionally filmed persons are not protected by the DPD, when using a video monitoring system, it need to be researched whether they might be protected under the second protection mechanism: the right to privacy (article 8 European Convention on Human Rights).

The right to privacy is, like the right to protection of personal data, interpreted very broadly by the European Court of Human Rights (ECHR). Moreover, it is one of the fundamental rights called upon most frequently. When assessing an alleged violation of the right to privacy, the ECHR takes into account the kind of information and the level of intimacy involved. As a consequence, the ECHR, in contrast to the DPD, makes a distinction between privacy sensitive and non privacy sensitive information. Therefore, not all data are equally protected. Seeing this distinction, I fear that the protection of occasionally filmed persons on the basis of right to privacy should not be taken for granted, despite the broad interpretation. This is because, although the images made do refer to the personal lives of the filmed persons, they might not be so intimate and might thus not so quickly be regarded as an unreasonable infringement as would with regard to the patient himself.

<sup>10</sup> See also Advice Belgian Commission for the Protection of the Privacy, June 7th 1995, n° 14, 6.

Furthermore, the ECHR also takes into account the doctrine of reasonable expectations of privacy. This doctrine originates from the US, where it was introduced in 1967 by Justice Harlan<sup>11</sup>. According to Harlan, privacy only needs to be protected, when there is an actual expectation thereto, and this expectation is regarded as reasonable by society. The reasonable expectations doctrine is, however, not interpreted in the same way in Europe as it is in the US: the ECHR has e.g., at least for now, only used this doctrine in cases of public privacy. With regard to the use of cameras, the ECHR has already decided that a person cannot call upon his or her right to privacy when filmed by surveillance cameras in a place where one could expect this to happen<sup>12</sup>. However, as it is typical for the concept of reasonable expectations, this is subject to change. The future will thus have to show how this concept will be interpreted, when cameras are used inside homes and of course each individual situation will necessitate a case-by-case approach.

## 4 The right of personal portrayal

The right of personal portrayal means that every natural person has the right to his or her own images and the right to keep them. This means that permission must be granted to create any human portrait, and for every use of one.

The right of personal portrayal is in fact part of the right to a private life, which in turn is part of the right to privacy. The right of personal portrayal is protected by article 8 of the European Charter on Human Rights, article 17 of the International Covenant on Civil and Political Rights, and by many Constitutions such as Belgium's (article 22 Belgian Constitution).

### 4.1 Scope of the right to personal portrayal

The scope of the right to personal portrayal is fairly broad.

First of all, the right to personal portrayal is both an individual and a family right. On the one hand, the individual right protects the personal portraits of all natural persons just because they are human beings (Dierickx, 2005). On the other hand, the familial privacy or familial integrity right protects the fellow humans of the portrayed person (Gukdix, 1980-81). However, an infringement of the familial right of personal portrayal is often not accepted in the jurisprudence. The cases in which such an infringement has been accepted were always sexually orientated.

Secondly, both the image and the portrait of a person are protected. This implies that both the physical features and the behavior of a person are included. Among examples from the jurisprudence of what is protected are the special way of clothing, the general conduct of a person, and memories of certain habits. Examples of what is not protected by the right to personal portrayal are the characteristics of a person or his or her voice. The voice of a person is, however, protected by a different right, namely the personal right to the voice (Senave, 2004).

Thirdly, an image or portrait can be made with all kinds of different technologies: two-dimensional photos and films, as well as three-dimensional sculptures, are protected. Furthermore, it is of no importance whether the portrait exists in a physical form, or is immaterial (e.g. live stream of a camera).

<sup>11</sup> in the well known Katz vs. United States case ruled by the U.S. Supreme Court.

<sup>12</sup> Lódi v Switzerland, EHRM June 15th 1992, <http://cmiskp.echr.coe.int/tkp197/view.asp?item=27&portal=hbkm&action=html&highlight=&sessionid=10078018&skin=hudoc-en>; Halford v United Kingdom, EHRM June 25th 1997, <http://cmiskp.echr.coe.int/tkp197/view.asp?item=1&portal=hbkm&action=html&highlight=&sessionid=10078018&skin=hudoc-en>; See also Loermans, 2004.

Apart from these three broadening elements, there is one limitation to the right of personal portrayal, namely, that the person is only protected when he or she is recognizable. How the term “recognizable” must be interpreted depends on the sovereign opinion of the judge, but it is advisable to take into account the same rules as used in the DPD. Recognizability must always be regarded from the point of view of others, and not the person in the portrait; however, being recognizable to friends and / or family is sufficient to invoke the protection (Dierickx, 2005).

## 4.2 Protection of the right to personal portrayal

When a person believes that his or her right to personal portrayal has been infringed, he or she can invoke his or her right against every person, who “makes” or “uses” the portrait without consent. This is what is called the erga omnes effect.

What comprises the “making” of a portrait has already been cleared out above: it concerns every image made by no matter what technology, and captured in no matter what way. However, what comprises “using” a portrait is less clear. In the legal doctrine, there is, e.g., discussion whether or not the use must have a commercial purpose. In the Belgian jurisprudence, the need for a commercial purpose has, however, not (yet) been accepted (Dierickx, 2005).

All actions considered as using a portrait can only be rightful after obtaining consent. Naturally, of course, whatever is not considered to be using a portrait can be done without consent. It has to be stressed that consent to make a portrait is not the same as consent to use a portrait, nor to reuse a portrait. So, in the case of the use of cameras inside people’s homes, different consents need to be obtained in order to monitor the patient, in order to store the images made, and in order to transfer the images, e.g., to a health professional. In addition, a presumed consent will never be accepted in the case of the reuse or reproduction of a portrait.

For the consent there are, of course, certain conditions on how this should be obtained and on what information it should be based, but this issue goes beyond the subject of this paper.

## 5 Conclusion

When cameras are placed in people’s homes, the images made can be protected by three different legal mechanisms: the protection of personal data, the protection of the right to privacy, and the protection of the right to personal portrayal.

Images and sounds from a patient made with an observation camera are protected by the Data Protection Directive. There is, however, discussion about the images and sounds of occasional visitors. Some people regard the purpose of the filming as the decisive criterion. Others, on the other hand, only take the purpose of the processing into account when assessing the lawfulness thereof, and regard every image of an identified or identifiable person as the processing of personal data. Discussion also arises with regard to the qualification as sensitive data. The processed data of the patient are most likely to be qualified as health data, and thus protected under the regime of sensitive data. Data of occasional visitors are, in contrast, most likely not to be thus qualified.

The protection of personal data is however only part of the protection of the right to privacy. For patients, the right to privacy will undoubtedly be part of the game. With regard to occasional visitors, however, this is not so likely due to the interpretation of the right to privacy by the ECHR.

Last but not least, the images will also be protected by the right to personal portrayal when filmed people are recognizable. The right to personal portrayal is interpreted in a fairly broad way.

Due to these three protection mechanisms, the use of cameras as a next step in eHomecare will currently have to be based on the consent of the patient. Whether or not occasional visitors need to be warned about the use of cameras in the homes they are visiting, though, is still open for discussion. However, in my personal opinion, I tend to say this would be necessary too. In what way this warning must be given and how realistic this is, are two further questions to which the answers will most likely depend on the national laws of the different member states.

## 6 REFERENCES

Bullesbach, A., Poulet, Y. and Prins, C. (2006). *Concise European IT Law*, The Netherlands: Kluwer Law International.

Bygrave L.A. (2002). *Data Protection Law: Approaching its Rationale, Logic and Limits*, The Netherlands: Kluwer Law International.

Dierickx, L. (2005). *Right to personal portrayal*, Antwerpen: Intersentia. (In Dutch)

Senaeve, P. (2004). *Compendium of personal and familyrights*, Leuven: Acco. (In Dutch)

Coudert, F. and Dumortier, J. (2008). *Intelligent video surveillance networks: data protection challenges*. Proceedings of The Third International Conference on Availability, Reliability and Security (ARES'08), 4-7 Mars 2008, IEEE Computer Society, 975-981.

Gukdix, E. (1980-81). *General systematical considerations about the right to personal portrayal*. *Rechtskundig Weekblad*, 47-50. (In Dutch)

Loermans, R. (2004). *Privacycolloquium 'Reasonable expectations of privacy'*, *Privacy & Informatie*, 161 (4). (In Dutch)

### Authors

#### Griet Verhenneman

Legal Researcher ICT

ICRI - K.U.Leuven - IBBT

[griet.verhenneman@law.kuleuven.be](mailto:griet.verhenneman@law.kuleuven.be)

<http://www.epractice.eu/en/people/12892>



The European Journal of ePractice is a digital publication on eTransformation by ePractice.eu, a portal created by the European Commission to promote the sharing of good practices in eGovernment, eHealth and eInclusion.

Edited by:  
EUROPEAN DYNAMICS SA

Web: [www.epracticejournal.eu](http://www.epracticejournal.eu)  
Email: [editorial@epractice.eu](mailto:editorial@epractice.eu)



The texts published in this journal, unless otherwise indicated, are subject to a Creative Commons Attribution-NonCommercial-NoDerivatives 2.5 licence. They may be copied, distributed and broadcast provided that the author and the e-journal that publishes them, European Journal of ePractice, are cited. Commercial use and derivative works are not permitted. The full licence can be consulted on <http://creativecommons.org/licenses/by-nc-nd/2.5/>