BIOMETRIC IDENTITY VERIFICATION IN HEALTH SERVICES: A BIOMETRIC SURVEILLANCE PRACTICE IN TURKEY

SAĞLIK HİZMETLERİNDE BİYOMETRİK KİMLİK DOĞRULAMA: TÜRKİYE'DE BİYOMETRİK GÖZETİMİN BİR UYGULAMASI

İlker ŞİRİN*

ABSTRACT

Determination or verification of identity with biometric methods has a widespread use especially at borders for security reasons. Social Security Institution transferred the biometric identity verification practice to health sercives that are provided by private and university hospitals. The risks of the new system considering the privacy of personal data are under debate. Although there are announcements or manuals of Social Security Institution regarding the implementation and legislation for data sharing and security exists, lack of a national data protection law brings with it security gaps.

Keywords: biometric verification, state surveillance, health services.

ÖZET

Biyometrik yöntemlerle kişilerin kimliğinin tespiti veya doğrulanması, güvenlik nedenlerine bağlı olarak özellikle sınırlarda yaygın olarak kullanılmaktadır. Sosyal Güvenlik Kurumu, biyometrik kimlik doğrulama uygulamasını özel ve üniversite hastaneleri tarafından sunulan sağlık hizmetlerine taşımıştır. Sistemin kişisel bilgilerin mahremiyeti açısından riskler barındırdığı tartışma konusudur.

* Sosyal Güvenlik Uzmanı, Sosyal Güvenlik Kurumu, Aktüerya ve Fon Yönetimi Daire Başkanlığı, Ziyabey Cad. No:6 Balgat/ANKARA, isirin@sgk.gov.tr, 0312 207 87 02

Sosyal Güvenlik Kurumu'nun uygulamaya ilişkin kılavuz ve duyuruları ile veri paylaşımı ve güvenliği konusundaki mevzuatı mevcutsa da, ulusal bir veri koruma kanununun hazırlanmamış olması güvenlik boşluklarına neden olmaktadır.

Anahtar kelimeler: biyometrik doğrulama, devlet gözetimi, sağlık hizmetleri.

1. Background

Biometric identification is an umbrella term for technologies matching live image of a body part with the previously recorded image of the same part. In other words, body is used as an identifier of individual. Some biometric identifiers are: digital fingerprints, retinal scans, hand geometry, facial characteristics and voice (Alterman, 2003; p.139).

In Turkey, some part of health service provision to universal health insurance (UHI) holders under social security is sustained via the biometric identity verification system (BIVS) since 1/7/2012. The BIVS, has started with pilot studies in Konya and then some additional provinces joined. The system is gradually widespreading nowadays. Every UHI holder, when visiting private health service providers (HSPs) are obliged to present palm vein print scanning or finger vein print scanning to verify their identities. It is not possible to be treated without passing through the BIVS. Similarly, Social Security Institution (SSI) does not pay for the services to HSPs that are not included in the BIVS. Currently private HSPs are under coverage but university hospitals will also be included as at 1/9/2014.

Recently, the BIVS was subject to adjudication by non govermental organisation of physicians-Turkish Medical Association. In summary, the association claims that the BIVS practice is against privacy rights and not in line with Turkish Constitution requirements (TTB, 2014).

The implementation of BIVS is simple. As the patient goes to HSPs, the biometric data is received at registration. There is a printed form denoting the Statement of Consent of the patient which should

be signed (by the patient) before the biometric data is received. Afterwards, during all visits to the HSP, firstly the patient is identified with ID, driving license, passport or marriage certificate and secondly, verification with the BIVS is done by palm vein print scanning or finger vein print scanning. For every phase considering treatments that need repetitive sessions such as extracorporeal shock wave lithotripsy (ESWL), extracorporeal shock wave therapy (ESWT), dialysis, physiotherapy or hyperbaric oxygen treatment, biometric verification is repeated before starting every session (SSI, 2013).

Exemptions to the BIVS is possible for the following group of patients:

- Children below 12 and elderly above 65,
- Those without two upper extremities (both hands),
- Those with degenerative both palms or both hand finger vein prints,
- Emergency cases,
- Those with cerebral palsy, upper extremity stroke or any other medical reason not allowing to receive biomedical information.

The philosophy behind the BIVS is to guarantee (or verify certainly) that the person demanding health service is the one who is eligible to get the service and also can be verified with body in addition to ID, driving licence, passport or marriage certificate. In other words, the BIVS is designed to prevent unjust use (abuse as well as fraud), i.e. receiving services as if one another.

Use of the new system is also reasoned by SSI to prevent abuse and fraud or prevention of unfair use of health services by ineligible people. On the other hand, the new system in our country also needs to be discussed considering prevention of personel data and privacy right which are critical issues of biometric identification in recent literature (Krasmann and Kühne, 2014, p.5; Çavlin Bozbeyoğlu, 2011; Graham and Wood, 2003, p.16; Bowyer, 2004; Alterman, 2003, p.140).

In that sense, this study attempts to highlight biometric verification in Turkey specifically for health insurance, which is a new and unstudied topic currently.

1. 1. Objective and research questions

In this study the aim is to discuss the biometric identity verification system (BIVS) practice in health services and evaluate Turkish practice considering protection of personel data. We are interested in the BIVS which is used by SSI since 1/7/2012 considering second level private hospitals i.e. hospitals both for in-patient and out-patient services.

The following research questions are studied:

(1) What is the role of biometric systems in state surveillance?

(2) How and with which steps is the BIVS implemented in health services for Turkey?

(3) What risks does the BIVS have considering protection of personal data and reaching health?

(3.1) What is the data protection system?

(3.2) With whom is data shared?

1.2. Recent literature

Collection of information about individuals is usually attributed to modern Western state. According to Higgs (2001), although not systematic and central, data on individuals always used to be gathered since pre-modern England. Church records provide the early versions of decentralised information system. Headcounts for military purposes or land ownership (and production) are other types of data that is collected. The author claims that state surveillance is not a new social function. Biometrics or other types of electronic systems in identification are the modern versions of traditional surveillance practices.

In recent literature, the identity verification and e-government applications in Turkey are critised because of data security, and practices ignoring privacy rights (Ketizmen and Ülküderner, 2007).

There are also studies discussing biometric systems in the European context. Alterman (2003), handles biometric systems with special emphasis on ethical issues and privacy right. He discusses four main risks of biometrics.

- The individual loses the control over the information gathered via the body,

- The system has a potential of misuse risk and safety becomes important,

- Unimaginable difficulties may arise in case that the information is distributed,

- Without consent of the person, the biometric information can be shared with the entire world.

Bauer and Olsén (2009), perceive medical surveillance as a tool and resource for epidemiologic research. They think that it is a useful element of modern diagnostics and helps decision making in the clinic. In another study, Krasmann and Kühne (2014), examine the biometric fingerprint practice of Germany which was fairly critised. The authors find digital fingerprints problematic because of their unforeseeble extended use.

Bright (2011), hopefully suggests that as more people will continue to live in democratic socities, surveillance technologies will be subject to democratic control.

1.3. Data and methods

To describe the basic implementation of BIVS in health insurances in Turkey, the current legislation that allows for receiving biometric data of UHI holders shall be determined. This descriptive study also analyses state surveillance using biometric systems and describes the recent practice of SSI in Turkey.

2. Findings

Role of Biometric Systems in State Surveillance

Biometrics, as a security measure, is firstly used in Mexican border (Velez, 2012, p.48). Country practices, especially after the September 11 attacks show that, biometric identification has a widespread use in terms of national security. Additional to the classical identification with ID or other proof, biometric verification may be used to guarantee that people are who they say they are, for instance in health care system. Thus, a second area of use considering biometric systems is to sustain system security. As an element of state surveillance, biometric systems render service to verification (or authentication) as well as identification (Zureik and Hindle, 2004, p.117). Lyon and Bennett (2008), provide detailed information on national ID cards around the world in which country specific biometric use is tabulated.

After September 11, biometric identification is preferred to conventional passports or classical proof of identification. Germany is one of the countries where biometric fingerprint is introduced as features of passports and identity cards after 2001. United Arab Emirates is another example to use of biometrics in border controls. Iris recognition started to be used in borders in 2003. Biometric systems in borders, makes risk analyses available and enables "identification before the event" (Krasmann and Kühne, 2014; Karake-Shalhoub, 2008, p.134; Amoore, 2008, p.24). Nation states in the international arena, need more in depth anaysis to sort out exactly "who is who" (Torpey, 1997, p.245). For security purposes, some border gates at UK such as Gatwick, Stansted and Manchester airports, biometric technology of face recognition is preferred (Bright, 2011, p.243). Home Affairs National Identity System (HANIS) in South Africa where photographic identification, biometric registration and smart card applications are applied together, Alien Registration Card of Japan since November 2007 by which fingerprinting instead of ink and paper, are other country practices (Breckenridge, 2008, p. 41; Ogasawara, 2008, p.94). It is clear from country practices that use of biometric systems in state

surveillance is motivated via national security needs and its role is expanding with improving technology.

Steps of BIVS Practice in Health Services for Turkey

In the Turkish context, the BIVS is rather new in health service provision but its capacity is improving to cover all type of health information in the country.

Before discussing the process of the BIVS, touching upon the legislative background may help to better understand the system in Turkey.

In 2010 Turkish Constitution was subject to an amendment. The third paragraph of Article 20 proposes regulations on privacy. According to the new rules the following can be highlighted:

- Everbody has the right to desire protection of personal data.

- This right covers; getting information on content of data, accessing the data, demanding to correct or delete the data and learning if the data is used according to purposes of gathering the information.

- Personal data can only be processed in certain conditions defined by law or explicit consent of the individual.

- Principals and methods with regard to protection of personal data should be prescribed by law (Constitutional Court, 2014).

According to the Constitution, SSI had to amend the Law-5510, i.e. Social Insurances and Universal Health Insurance Law before the introduction of BIVS. Therefore, the third paragraph of Article 67 of 5510 was amended with the Law-6283 dating 1/3/2012. The new version of the article brings with biometric verification as an option for authentication of identity before receiving health services (Prime Ministry, 2014). In line with legislative hierarchy, Health Implementation Rules of SSI was also revised in order to adapt to the biometric verification. Lines 1.6 and 1.6.1 which are about “Determination of identity” and “Biometric identity verification” were renewed. The third paragraph of line 1.6 emphasises that, in case anyone has

responsibility on letting health services available to those who are not eligible, shall pay two times the unjust cost to SSI. In addition, those taking part in such actions shall be punished according to the Turkish Penal Code rules. After the legislative preparation phase, soon after the Law 6283 in March 2012, SSI introduced pilot implementation of biometric verification in health services in a province of Turkey, Konya in July 2012.

In Konya, second level private HSPs including private hospitals and medical centres giving services were under coverage. Then, in 15 September 2012, the system was adapted in 20 new provinces.[1] Interestingly, Bolu, where the pilot studies of electronic ID card (2008) including biometric features is not chosen as a province in the preliminary implementation period by SSI. As touched upon by Çavlin Bozbeyoğlu (2011), the goal of electronic ID was universal coverage and it was planned as a widespread tool in various public processes including social security.

As at 1 December 2013, private HSPs in the remaining 60 provinces started to use the BIVS. Since that date, no provision over MEDULA (a soft ware of SSI that tracks all services provided to patients and payments to HSPs) was given to HPSs meaning inability to give services to the UHI holders or get payments from SSI (SSI, 2013a). However, during transition, some HSPs declared problems with regard to adaptation to the new system. Therefore exemptions were also possible. If the HSP had used BIVS at least one time before 31 December 2013, they were allowed to use MEDULA system without BIVS for restricted periods (SSI, 2013b).

Inclusion of university hospitals was subject to alterations for two times. Firstly, the plan was to cover them latest 1/4/2013, but due to unready HSPs, it was postponed to 1/9/2013. Finally SSI plans to cover university hospitals in the BIVS as at 1/9/2014 (SSI, 2013c).

In summary, there is a rapid and pervasive growth in the BIVS practice in Turkey.

1 Ağrı, Amasya, Bartın, Bilecik, Bingöl, Bitlis, Burdur, Çankırı, Iğdır, Karabük, Karaman, Kastamonu, Kilis, Mardin, Muş, Nevşehir, Niğde, Sinop, Şırnak, Yozgat

Risks of BIVS

Although there is a rapidity in the BIVS practice, the robustness of the system is questionable. Current legislation as well as the announcements of SSI for instructing HSPs imply that main focus of SSI is prevention of unjust payments.

It was announced by SSI that it is the responsability of HSPs; to use devices in line with requirements in Terms of Reference (ToR), otherwise related security gaps and breakdowns resulting with public loss to SSI should be covered by HSPs. Currently, there are 5 companies sustaining the requirements in the ToR declared by SSI and are eligible to provide the biometric scanning devices (SSI, 2013d).

Device type is an important element of security. In the manual of SSI, one type of device for palm vein print scanning and four types devices for finger vein print scanning is presented in the annex. Only for palm vein print scanning devices, it is a prerequisite that the processing unit should be in line with the "Directive 95/46/EC of The European Parliament and of The Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data" (SSI, 2013; European Commission, 1995).

The Turkish Constitution proposes that issues related with protection of personal data should be prescribed by law. However, as Turkey does not have a Law on data protection, SSI found a solution by preparing a Memorandum on authorization of staff for different operations. European Commission (2013) criticizes the gap in legislation regarding data protection. The recent Proggress Report highlights the current situation in Turkey with following statements "*There have been no significant developments as regards the protection of personal data. Turkey has yet to adopt a general law on the protection of personal data and, in that context, to set up a fully independent data-protection authority.*" (European Commission, 2013, p.63). Thus, the memorandum of SSI is the only legal document specifically designed to authorize three levels of operations under the BIVS.

According to the memorandum, only SSI staff in the center or province organisation has the right to pass queries. In other words only SSI can track the information received by the BIVS. SSI staff can report the citizen operations as well as HSP and out-patient clinic specific information. The authorization is for operations related with;

- Controling the records,
- Deleting the records in necessity,
- Statistical data and reporting.

Therefore, the BIVS also allows for deleting the record in the database. Deleting the BIVS record can be demanded by the patient or the HSPs. Demand can also be sent by facsimilie message. HSPs have to send their request for deleting the record to Social Security Province Directorate (SSPD) where the HPS is operating or to the SSPD the invoices are received by. If the patient wants to delete the record, information on ID, address, phone number and reason of deletion is also included. In addition to the aforementioned information HSPs should give details regarding institution code and name (SSI, 2013e).

Data sharing with third bodies is also regulated by SSI. In 2012, SSI declared a document for principals and methods of data sharing. In case of data demand, the commission under SSI decides if the demanded data can be shared or not. Personal data is defined as “secret data” in the document and it is not subject to sharing with other bodies. In addition, Article 12 of the Principal and Methods proposes that HSPs also have responsibility in securely keeping the data of UHI holders in their units. They are not allowed to share the data with any other body without the permission of SSI.

The other risk of the BIVS arises when trying to reach health services. The system seems to be voluntary in the sense that the consent of the patient for the BIVS is received at the beginning. However, the person at the registration desk in a hospital is bounded and has no chance other than signing the form.

3. Conclusion

The objective of this paper was to discuss the biometric identity verification system in health service provision in Turkey. Biometric systems are widespreading in all regions around the world. Such systems are especially used during border controls. The BIVS practice in health insurance in Turkey is relatively new but it has a pervasive character. University hospitals will be included in coverage soon. The system has potential risks regarding privacy. The focus of SSI is on costs, sustainability and commercial priorities rather than privacy and ethics. Although SSI has regulations and efforts to sustain data security and has rules of information sharing, lack of a national data protection law leaves many gaps in the biometric verification system.

REFERENCES

Alterman, A. (2003), 'A piece of yourself'': Ethical issues in biometric identification'. Ethics and Information Technology 5: 139–150.

Amoore, L. "Governing By Identity". In Playing the ID card: Surveillance, security and identity in global perspective, edited by Colin Bennett and David Lyon, 21-36. London: Routledge, 2008.

Bauer, S. and J.E. Olsén (2009), 'Observing the Others, Watching Over Oneself: Themes of Medical Surveillance in Society'. Surveillance&Society 6(2): 116-127.

Bowyer, K. W. (2004), 'Face Recognition Technology and the Security Versus Privacy Tradeoff'. IEEE Technology and Society, Spring 2004, 9-20.

Breckenridge, Keith. "The Elusive Panopticon: The HANIS Project and the Politics of Standards in South Africa." In Playing the ID card: Surveillance, security and identity in global perspective, edited by Colin Bennett and David Lyon, 39-56. London: Routledge, 2008.

Bright, J. (2011), 'Building Biometrics: Knowledge Construction in the Democratic Control of Surveillance Technology'. Surveillance&Society 9(1/2): 233-247.

Constitutional Court (2014), 'Turkish Constitution' (Turkish).

Çavlin Bozbeyoğlu, A. (2011), 'Citizenship rights in a surveillance society: The case of the electronic ID card in Turkey'. Surveillance&Society 9(1/2): 64-79.

European Commission (1995), 'Official Journal L 281 , 23/11/1995 P. 0031 – 0050'. Internet: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri =CELEX:31995L0046:en:HTML. Last visited on June 11, 2014

European Commission (2013), Turkey 2013 Progress Report-SWD(2013) 417 final.

Graham, S. and D. Wood (2003), 'Digitizing Surveillance: Categorization, Space, Inequality'. Critical Social Policy 23(2), 227-248.

Higgs, Edward (2001), "The Rise of the Information State: the Development of Central State Surveillance of the Citizen in England, 1500-2000", Journal of Historical Society, Vol. 14 No.2.

Internet: http://www.anayasa.gov.tr/Mevzuat/Anayasa1982/. Last visited on June 9, 2014.

Karake-Shalhoub, Z. "Population ID card systems in the Middle East: The cas of the UAE". In Playing the ID card: Surveillance, security and identity in global perspective, edited by Colin Bennett and David Lyon, 128-141. London: Routledge, 2008.

Ketizmen, M. and Ç. Ülküderner (2007), "E-Devlet Uygulamalarında Kişisel Verinin Korunma(ma)sı", XII. Türkiye'de İnternet Konferansı, 8-10 Kasım 2007, Ankara: İnternet Teknolojileri Derneği. Internet: http://inet-tr.org.tr/inetconf12/bildiri/2.pdf. Last visited on June 13, 2014.

Krasmann, S. and S. Kühne (2014), ''My fingerprint on Osama's cup'. On objectivity and the role of the fictive regarding the acceptance of a biometric technology'. Surveillance&Society 12(1): 1-14.

Lyon, D. and C.J. Bennett (2008), "Playing the ID card: Understanding the significance of identity card systems". In Playing the ID card: Surveillance, security and identity in global perspective, edited by Colin Bennett and David Lyon, 3-20. London: Routledge, 2008.

Prime Ministry (2014), 'Prime Ministry-Legislation Information System: e-legislation' (Turkish). Internet: http://www.mevzuat.gov.tr/Kanunlar.aspx. Last visited on June 9, 2014.

SSI (2013), 'Manual for Identity Verification with Biometric Methods' (Turkish). Internet: http://www.sgk.gov.tr/wps/portal/tr/e_sgk/diger_uygulamalar/duyurular. Last visited on June 1, 2014.

SSI (2013a), 'Announcement of 27/11/2013' (Turkish). Internet: http://www.sgk.gov.tr/wps/portal/tr/e_sgk/diger_uygulamalar/duyurular. Last visited on June 6, 2014.

SSI (2013b), 'Announcement of 10/1/2014' (Turkish). Internet: http://www.sgk.gov.tr/wps/portal/tr/e_sgk/diger_uygulamalar/duyurular. Last visited on June 8, 2014.

SSI (2013c), 'Announcement of 22/3/2013' (Turkish). Internet: http://www.sgk.gov.tr/wps/portal/tr/e_sgk/diger_uygulamalar/duyurular. Last visited on June 9, 2014.

SSI (2013d), 'Announcement of 25/11/2013' (Turkish). Internet: http://www.sgk.gov.tr/wps/portal/tr/e_sgk/diger_uygulamalar/duyurular. Last visited on June 9, 2014.

SSI (2013e), 'Announcement of 20/9/2013' (Turkish). Internet: http://www.sgk.gov.tr/wps/portal/tr/e_sgk/diger_uygulamalar/duyurular. Last visited on June 10, 2014.

Torpey, J. (1997), 'Coming and Going: On the State Monopolization of the Legitimate "Means of Movement"'. Sociological