The Meaning of the SWIFT Provisional Agreement for the EU – US Partnership, with a Focus on Counterterrorism and Data Protection

Ramona Ricarda POPA
Serviciul Român de Informații
e-mail: **ricarda_popa@yahoo.de**

Executive summary:
The SWIFT agreement between the US and the EU is an instrument meant to facilitate the fight against terrorism by sharing data on electronic value transfers. It came into discussion after the 9/11 attacks and the indignation caused by the secret access of some US institutions to personal and financial records of EU citizens. The Agreement represents a challenge to the two great soft powers since its effects go beyond the initially declared cooperation purpose, dealing also with the sensitive issue of protection of personal data, which makes it of direct interest to almost every EU citizen. On a global level, it casts a new light on the transatlantic relationship as it reflects different concepts of state and people security. On a continental level, it shows internal EU divisions of procedural and legal nature as well as a cooperation-deficit between EU institutions, representing a challenge for law makers, security experts, and law enforcement authorities. On individual level, the SWIFT affair certainly raises questions regarding the free exchange of ideas, news, goods and services, etc.

Keywords: SWIFT, counterterrorism, Terrorist Finance Tracking Program, data protection, data manipulation, personal data transfer, electronic value transfer, EU, U.S. Treasury Department, Safe Harbor, transatlantic partnership, security affairs.

1. Introduction

1.1 The factual background

The SWIFT Agreement is an accord between the European Union and the United States of America regarding the processing and transfer of Financial Messaging Data from the EU to the US for the purposes of the

Terrorist Finance Tracking Program[1]. The Agreement has emerged out of the desire of the parties "to prevent and combat terrorism and its financing, in particular by mutual sharing of information, as a means of protecting their respective democratic societies and common values, rights, and freedoms"[2], in the spirit of the transatlantic partnership, based on the UN Security Council Resolution 1373[3]. Its purpose is to ensure that the concerning data "are made available upon request by the U.S. Treasury Department[4] for the purpose of prevention, investigation, detection, or prosecution of terrorism or terrorist financing." (Agreement, § 1.1a) Signed on November 30,2009, the Agreement goes into effect on February 1,2010 for an agreed period of 9 months, and represents an interim solution until a long-term agreement is ratified.

SWIFT is the abbreviation for the cooperative Society for Worldwide Interbank Financial Communications, founded in 1973 with the headquarters near Brussels, Belgium. It is based on Belgian law and has set the international common standards regarding worldwide financial transactions. Likewise, it has established a shared data processing system and worldwide communications network. SWIFT has been providing the proprietary communications platform, products and services that allows to connect and to exchange financial information securely. According to the

[1] It was created by the Bush Administration as a response to 9/11. It is conducted by the CIA, under the supervision of the Treasury Department and based mainly on the SWIFT transaction database, after top officials exerted pressure for the data transfer.

[2] See Agreement text.

[3] Signed September 28, 2001 to enhance international intelligence sharing in the field of counterterrorism, respectively, to impede the movement, organization, as well as fund-raising activities of terrorist groups. It created the SC's Counter Terrorism Committee, to monitor compliance with these provisions.

[4] The Treasury Department is the executive agency responsible for promoting economic prosperity and ensuring the financial security of the US. It operates and maintains systems that are critical to the nation's financial infrastructure, and works with other federal agencies, foreign governments, and international financial institutions to encourage global economic growth, and to predict and prevent economic and financial crises. It performs a critical and far-reaching role in enhancing national security by implementing economic sanctions against foreign threats to the U.S., identifying and targeting the financial support networks of national security threats, and improving the safeguards of our financial systems. Thus, it is the steward of U.S. economic and financial systems, and an influential participant in the global economy. (US Department of Treasury http://www.ustreas.gov/education/duties/)

official site of SWIFT, nowadays, over 8,300 financial institutions and banking organizations, security institutions, and corporate customers in the entire world employ it daily to exchange millions of standardized financial messages, stored for 124 days on a main and a backup computer server. (http://www.swift.com/) This represents about 80% of the worldwide traffic for electronic value transfers, according to the background note of the Justice and Home Affairs Council (p.5). Thus, due to its assignment and possibilities, SWIFT has become the first messaging service for banks issuing international transfers[5].

In June 2006, a series of articles published by The Wall Street Journal[6], The New York Times[7], and The Los Angeles Times[8] disclosed that after the 9/11 attacks, the Treasury Department, the FBI and the CIA had been accessing secretly and systematically the SWIFT database in Virginia, US, without individual court-approved warrants and without the knowledge of the European authorities, to examine the respective transactions[9] – based on a private agreement between SWIFT and the Treasury -, in order to capture al-Qaeda members suspect of having been involved in terrorist bombings. The publications had major consequences upon all 3 involved parties: first, SWIFT became member of Safe Harbor[10] to legalize the transfers, then, starting with December 31, 2009, the computer servers would move out to Switzerland. Finally, after investigations and 2 years of discussions, the SWIFT agreement was signed, to meet the US requirements for access to the data, and to ensure "that designated providers of international financial payment messaging services make available to the

[5] It is known by the customers by the SWIFT-BIC code, which is the SWIFT ID.

[6] It is the most distributed paper in the US, and adopts a more conservative, critical tone. Despite of this, the news tends to be rather liberal. Nonetheless, Gordon Crovitz, a former publisher of the paper, endorses the editors' pursuit for impartiality.

[7] It is the third most distributed daily US newspaper, and the largest metropolitan one, with partly conservative, and partly, but predominantly, liberal bias.

[8] It is the second-largest metropolitan newspaper, and the 4th most distributed in the US. It adopts a liberal tone.

[9] Here one can see the 2 fears of the liberals: government power and mob rule (in this case mass media rule).

[10] Safe Harbor is an agreement employed initially for commercial purposes by economic agents that wanted to use the US as a hub in order to centralize their international data transfers. (Kuner 2009:4)

US Treasury – as administrative authority - financial payment messaging data stored in the EU, necessary for preventing and combating terrorism and its financing". (Preamble, 2nd paragraph) The request is to be executed as a matter of urgency and data may include information about the originator and/or recipient of the transaction, like name, account number, address, national identification number, and other personal data related to financial messages. (§ 4.2) Yet, the SWIFT transfers do not regard US citizens, as the database does not contain information on ordinary transactions that would be made by individuals in the US, such as deposits, withdrawals, checks, or electronic bill payments, according to Stuart Levey, an Under Secretary at the Treasury Department. (Levey, 2006)

The 2006 as well as the 2009 context brought forth a high degree of discontent among the EU representatives, since they regard this development as a US endeavor to achieve its own security goals, and because the US intelligence agencies have now more or less legal access to the personal, financial records of many EU citizens, using different data protection practices than the EU. The ongoing debate has three main critical dimensions, evolving on political-geostrategic, legal-procedural and security level.

1.2 The structural and analytic approach

The subsequent analysis is composed of three interconnected parts, which attempt to answer the question: "what is the impact of the Agreement for the EU-US relationship, in terms of counterterrorism and data protection?" The question is approached by a liberalist understanding of human security as elaborated by UNDP[11], and has takes as a legal frame the EU Data Protection Directive 95/46/EC, the European Convention on Human Rights § 8, the EU Charter of Fundamental Rights § 8, the US Safe Harbor, and the provisional SWIFT Agreement.

The first chapter focuses on the positioning of the two superpowers towards each other as security providers in a globalised world, starting from the utilization of the SWIFT resource. I consider this item of key importance, since the policies of the two entities are highly reflected in both security issues that are discussed in the following chapter. The second part deals with the dilemma of data transfer vs. the principle of respect for

[11] See: New dimensions of human security. In: Human Development Report 1994. Chapter 2. (http://hdr.undp.org/en/reports/global/hdr1994/).

privacy. The last part is concerned with the question of data transfer for an efficient anti-terror fight, the two sections trying to see what impact the agreement has on both data protection and counterterrorism.

According to the UNDP definition, security is no longer a narrow state-centered national issue, but has turned universal, integrative, people-centered, being understood as an all-encompassing concept of human security, since frontiers are no longer barriers, and threats come rather from the actions of millions of people than from aggression by a few nations. (UNDP 1994:24,34) Human security includes highly interdependent components – economic security, food security, health security, environmental security, personal security, community security, and political security – being easier to ensure through prevention (UNDP 1994:22).

I chose a liberalist understanding of human security because it offered more adequate analytical tools than other approaches: in a globalised world the variety of actors are dependant on cooperation to achieve the biggest gains. In international relations liberalism is one of the greatest advocates of interdependence and international cooperation based on a set of common values, in both high and low politics. The theory as it is found in the Oxford Manifesto of 1947 postulates that state preference determines state behavior, every individual having the right to enjoy the essential human liberties, the free exchange of ideas, news, goods and services. Censorship, protective trade barriers, and exchange regulations are rejected. Likewise, debates can be introduced by any actor. (www.liberal-international.org/editorial.asp?ia_id=535)

I applied a qualitative method of analysis, based on a close reading of the most complex press articles I could find on the *SWIFT affair*, both in the US and the EU, in English and German language. The French and Spanish speaking areas have been covered less by articles on this issue. The articles I found have a conservative, liberal or critical stance. Unfortunately I could not find any academic approach to the Swift Agreement until the moment of writing this paper, and only very few on the SWIFT scandal of 2006.

2. The EU-US bilateral relationship in the light of the new agreement

The presence of the SWIFT backup computer server on US territory has given the US security agencies unlimited access to sensitive data, offering them a considerable advantage over other countries in the fight

against terrorism, "a unique and powerful window into the operations of terrorist networks", as Stuart Levey declared. (Lichtblau 2006) Among these are the *link analyses* and their operative employment without individual warrants, a mandatory requirement within the EU. The above mentioned publications, disapproved by the US government, came as a radical bottom-up initiative, rejecting the US state-centric conception of security. Drawing the attention upon the unauthorized employment of sensitive EU resources and the breach against the privacy rights of the EU citizens, they emphasized the interdependency between development, human rights and national security, and called for a new settlement based on open cooperation. By doing this, a valuable top-down systematic prevention instrument was disclosed, striking heavily against a confidential strategy, not only because it taught the potential targets about its existence, jeopardizing ongoing operations and investigations, but also because it placed the US in a difficult position in front of the overseas partner.

The removal of the server from the US was initially seen as another blow to the US counterterrorist policy and thus as a weakening in front of the EU, since it was thought it would go far beyond being a mere change in the construct of this platform with a key role in the field of financial security. It meant restricting the US access to the transaction data because only the servers in the Netherlands and Switzerland[12] would process EU international payment transactions, which in turn meant that the US had to formulate legal, official requests for the records. Moreover, it would have created a certain degree of dependency on the concerned governments, thus decelerating the decision making process and reaction. To avoid this, the US government exerted massive pressure on Brussels, emphasizing the extensive nature of terrorism, based on the drop of the security levels that made the vulnerability against terrorist threats rise, including in Europe. The Secretary of State Hillary Clinton told her European counterparts the fate of the West hung in the balance, whereas US ambassadors "stormed EU governments pulling out all the moral and political stops." (Schlamp, 2009) In this respect, an Agreement would have allowed further access of the US to the SWIFT data, impairing less the usage of this vital tool that has played

[12] International standards and supervisory requirements ask that infrastructure is to be kept geographically separated.

for almost a decade a veiled part in the US national and international counterterrorist surveys and investigations.

After the initial fears were overcome by the US, the SWIFT Agreement turned out to be a tough nut to crack for the EU, as it implied inner European divisions between the EP and the EU Council, at the procedural and legal level. Although an international treaty or agreement requires the unanimous consent of all 27 members, the drafting process took place mainly behind closed doors, the EU Council infringing upon drafting and negotiation procedures, by eluding the EP. This happened even though many countries - especially Germany, Austria, France, and Finland - opposed vehemently to the Agreement, and are presently pushing for its suspension[13].

In this sense, after 2 years of discussions, the swiftly signed Agreement, just before the ratification of the Treaty of Lisbon, reflects the positioning of the two superpowers towards each other. First, it conveys a compromise of the EU towards the US, as well as a sign of trust, in order to keep the common strives against terrorism functioning. Second, it indicates that within the EU, foreign relations with its Western partner take priority to the necessity of solving internal fractures, whereas the US discourse maintained its own policy as a top priority This implies the EU has given in to the US pressure and requirements for the second time in this case, depicting the EU as actor on the international scene.

The SWIFT Agreement shows deficiencies in the internal EU cooperation as well as in the international cooperation realm, because signing the Agreement one or 2 days later, under the Treaty of Lisbon, would have meant harsher negotiating conditions for the US. This would have been based on more strict drafting and negotiating procedures since the EP would have had extensive co-legislative powers, and decision making competences in internal and security affairs, that is, it would have had the veto right. It would have meant a more extensive approach to such a sensitive issue like financial records transfers, since the Lisbon Treaty calls for more precise rules and more competences for the EP on data protection and fundamental rights regarding bank data transfer issues. By this means,

[13] Among them are Cornelia Ernst of Germany, Rui Tavares of Portugal, and Marie-Christine Vergiat of France, who are GUE/NGL MEPs on Parliament's Civil Liberties, Justice and Home Affairs Committee, the Alliance of Liberals and Democrats for Europe, etc.

the content of the Agreement has come to include a series of ill-defined aspects, the entire process shedding an unfavorable light on the EU compliance with democratic principles and upon its capacity for unitary decision making, keeping the EU in a critical position towards the US.

If the disclosure of SWIFT turning from a mere data processor to data controller[14] created in 2006 "legal and political clashes between Europe and the US" (Brand 2006), in 2010 the Agreement officializes this role, turning the EU into a bestower and the US into a beneficiary, with potential impairing consequences for the EU. On the **internal political** level, it cares for a restraint on European sovereignty. On the **financial-banking and data protection** level, it could bring forth monetary fines by banks, if the financial records of the clients are sent to the US government, without the existence of a well founded suspicion of terrorism. On the **security** level, it leaves unsolved the vulnerability for industrial and economic espionage by third parties, as long as the US conclusions based on a comprehensive analysis of financial data can be transferred to third parties.[15] Last, but not least, on the **level of international affair**s it keeps the EU in a position not to disturb in any way the relationship with the US, reflecting the unequal positions of the two involved parties.

3. Meaning for data protection

By accepting an unequal treatment on the basis of citizenship, through the lack of reciprocity, as well as the swift and undemocratic signing process, presuming that its postponing would have maintained the security vacuum, the interim Agreement did not succeed to impose itself against the highly determined US approach in international affairs. As the SWIFT affair depicts, the mere suspicion of a potential terrorist threat sufficed to legitimize protracted state action against the principle of privacy of financial data, recognized as a fundamental right within the EU. Without

[14] A data controller is a natural or legal person which alone or jointly with others determines the purposes and means of the processing of personal data, whereas a data processor is a natural or legal person which processes personal data solely on behalf of the data controller. EU Data Protection Directive § 2(d)-(e). Having this role, SWIFT violated the notification articles of the same directive.

[15] This is an issue discussed also within the Safe Harbor, the US-EU disagreements not having been solved yet.

a specific Congressional authorization (Lichtblau 2006) and without the knowledge of EU privacy commissioners, the US request of financial records corresponds to the infringement of the fundamental rights and the principles of democracy, because legal or institutional barriers to the government's access to private information have been trespassed. Some of the concerned EU bank institutions, who refused to support the US tactics in this respect, namely the European Central Bank, the National Bank of Belgium, the Bank of England and other G-10 banks, knowing about the data gathering, kept silence (Spongenberg 2009), supporting tacitly the US policy and outraging civil society.

The first major consequence of the SWIFT Agreement is that it limits the US access to sensitive EU personal financial data. Since the data would have to be processed and stored in the Netherlands and Switzerland, the US would have to address official requests, "tailored as narrowly as possible", to prevent too much consumer data from being evaluated by law enforcement and intelligence authorities. (Neely 2009) The second major consequence is that it acts upon the privacy[16] of banking data of EU businesses and citizens, because the Agreement actually cares for a shift from the US legislation to the EU one.

On the European continent, the financial personal data are considered human rights according to the European Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR), § 8, and the Council of Europe Convention No. 108 for the Protection of Individuals with regard to Automatic Processing of Personal Data. In the EU, these are protected by the Charter of Fundamental Rights of the EU and the EU Directive 95/46/ED, yet this does not cover the judicial and police cooperation, but it sees that data can only be *processed* with the consent of the data subject. The US does not have a comprehensive data protection system, so that basically an agreement in this sense automatically becomes a challenge and a potential source of tension between the two parties.

By this shift in the legislation field, the Agreement actually opens the way for a transatlantic harmonization of practices and data protection regulations, at higher protection standards, trying to set new rules for the US state behavior vs. state access to privacy. This means that the EU legal

[16] Westin sees privacy as the enforcement of people to determine when, how, and to what extent information about them is communicated to others.

framework takes a step towards gaining a central position in data sharing and that the use of the US governed *Safe Harbor* for security reasons also needs to be re-discussed. The official debates have not reached this point yet, since the EP has not been involved in the signing of the SWIFT Agreement, and the EU Commission, who indicated in 2007 that "onward transfers under Safe Harbor must fulfill the basic requirements of European data protection law" (Kuner 2009:4), has kept out of the signing affair.

On short term, the ongoing divergences around the transfer practices could have a rather hindering effect on the bilateral transatlantic cooperation in the field of data sharing for disclosing terrorist financing, since the legislation switch confronts the EU with two critical dilemmas in 2 fields of utmost importance for both sides:

- Is the transfer of personal financial information appropriate and proportional to the purpose of fighting terrorism, and transparent towards the financial customers?
- What is a too tight data protection and what is a too loose data protection?

Based concretely on the SWIFT Agreement, the first specific critical issues that created discontent refer to:

- the **manipulation standards** for personal financial information regarding the content of the data and their classification level:
    - regarding the **content** of the data, although the Agreement prohibits the onward transfer of data to third parties, broader conclusions based on these data could be passed indirectly to third parties, in the form of conclusions regarding markets, commercial partners, transaction volumes or price calculations and profit margin. Likewise, they could be used for other purposes, i.e. *risk assessment scores or economic profiling*. Financial Times Deutschland goes even further, assessing potential impacts on industrial and economic espionage. Therefore the Agreement is not only a legal consequence to the 'protectionist' call of restraining the US access to EU data, but embodies challenges for more specific limitations, since the "prevention, investigation, detection, or prosecution of terrorism or terrorist financing"[17] is a too wide-ranging

[17] See the Draft Agreement.

formulation to ensure the binding of the data to that purpose. Through this, it raises the proportionality question of the transfer, for how the data is connected to counterterrorist investigations has to be researched and explained first.

- regarding the **classification** level of the data, the Agreement raises the question of common data classification standards regarding EU sensitive and classified personal financial information. Practically, it determined privacy advocates to require that the US comply with the EU data protection standards when processing EU data, because EU beneficiaries should enjoy legal certainty. That means, on the one hand, that the US data protection level should not be lower than those in the EU. On the other hand, it means that a control mechanism should be used to check the compliance with the data protection rules. Under current rules, in the EU, each government is responsible for the application and enforcement of the common EU data privacy law.

- **Legal protection standards** of the data and of the citizens:
  - **The legal authorization** is mentioned only tangentially in terms of a 'central authority', which does not suit the EP demands. The procedures on who decides and how the **decision** is taken regarding the transfer and processing of the data for the purpose of fighting terrorism is too broadly defined.
  - the Agreement still allows an easy access to personal financial data without strong **judicial safeguards**, which raises questions regarding its appropriateness. Not requiring individual search warrants to access financial data violates the principles for privacy and the protection of personal data under the above mentioned EU laws. In this respect, the Agreement calls for more safeguards to prevent broader data searches, determining EU internal disagreements. The fact that the Agreement does not design a role for any data protection body caused Frank Rieger[18] to declare that the

[18] Spokesperson for the Berlin Chaos Computer Club, an organization that advocates online privacy.

Agreement is rather reflecting data imperialism, than an anti-terrorism deal. (Neely 2009)

- The agreement does not legally **protect the citizens against abuse**, since there is no judicial help or protection for "individuals believed to be acting as a "foreign terrorist agent". (Meyer 2006) The Agreement provides for the possibility that "any person who considers his or her personal data to have been processed in breach of this Agreement is entitled to seek effective administrative and judicial redress in accordance with the laws of the EU, its Member States, and the US, respectively" (art.11.3). Yet, there are no further provision regarding how an EU citizen could file a complaint against the US authorities over their handling of their personal data.

  At this point the Agreement reflects a major difference between the EU and US on data protection and privacy, which has produced clashes between the two parties. Whereas the EU follows a socially protective and proactive pattern, the US is rather reactive, being advantaged by the fact that privacy laws are enforced on banks not on banking consortiums like SWIFT.

- The **time limit** of the Agreement does not surpass 2010, whereas the data would be stored for 5 years, which makes the German Federal Criminal Police Office (BKA) doubt the use of the data in the fight against terrorism.

The development in the field of data transfer starting with the passenger name record and the US Customs and Border Protection, up to the SWIFT Agreement, calls for a serious reflection in the area of the data protection policies. This is not only because of the need for common principles and practices in a field in which the EU and the US collide while claiming world leadership. It is also due to the substantial disadvantage in front of the terrorist threat, as the most recent debates have shown: despite the amount of measures for the protection of common rights and values, lawmakers and law enforcers seem to have failed in adapting to the technological challenges.

4. Meaning for the counterterrorist fight

Gilles de Kerchove, the EU Counterterrorism Coordinator, alleges that SWIFT is indispensable for the counterterrorist fight, "one of the most valuable sources of information […] on terrorist financing", as Levey affirms, because it provides a rich *hunting ground* for investigations. As the information can be "mapped and analyzed to detect patterns, shifts in strategy, specific *hotspot* accounts, and locations that have become havens for terrorist activity" (Meyer 2006), the program has pointed to new suspects or "key links in the investigations of al Qaida and other deadly terrorist groups". (Levey, 2006). "Since the Sept. 11 attacks, it has tracked millions of confidential financial transactions handled by SWIFT." (Brand 2006 quotes the U.S. Treasury) "The value of the program has been in tracking lower- and mid-level terrorist operatives and financiers who believe they have not been detected and militant groups, such as Hezbollah, Hamas and Palestinian Islamic Jihad..." (Meyer 2006 quotes Stuart Levey) The SWIFT data has supposedly helped capturing the German 'Sauerland Group'[19], Hambali, the mastermind of the 2002 bombing in Bali, and breaking a terrorist network in the UK[20]; it has helped identify Uzair Paracha, an al Qaeda operative in Pakistan, etc. (Lichtblau 2006)

Nonetheless, the usage of SWIFT data for counterterrorist purposes did not correspond to the original, commercial processing purpose, violating the proportionality principle established by the 95/46/EC Directive. This aspect mirrors the conflicting situation of SWIFT before signing the Agreement: based upon EU legislation, its server in the US had to work under the US legal jurisdiction, being bound to respond to the administrative subpoenas; otherwise it made itself guilty of federal offence. Not infringing US civil rights meant infringing EU fundamental rights. The responsibility for this trespassing bears SWIFT, but also the informed EU financial institutions and banking organizations.

[19] The Group, captured in September 2007, was formed of three Germans converted to Islam and a Turk: Fritz Gelowicz, Daniel Schneider, Attila Selek, Adem Yilmaz. The group was part of the Islamic Jihad Union that has contacts with al Qaida. Their plan was to attack several US facilities in several German cities, by means of car bombings.

[20] Abdulla Ahmed Ali, Tanvir Hussain, and Assad Sarwar conspired to activate bombs disguised as drinks in order to blow up planes flying fron London to US. They were convicted for 30 years; another 4 were found not guilty.

Placing both SWIFT servers under EU legislation for complying with the EU legal framework, may bring about at least a tactical change in the US data collection policy in the field of cutting terrorism financing overseas, since it may induce a deceleration in the analysis based upon SWIFT data. Before the Agreement, TFTP had direct unrestricted access to the data, based on a monthly administrative subpoena[21], without having to seek assistance from foreign banks. This prevented potential time lags or refusals of cooperation. (Meyer 2006) The Agreement changes this situation since it "limits the US authorities' information requests to people with [proven] links to terrorist activity. First, the US authorities must justify their requests with the US Treasury, and then, they must structure them to be as specific as possible, because otherwise, any EU citizen could become object of the US investigators." (Lawton 2009)

This makes indirectly the Agreement require more than an Automated Targeting System[22], and that the various levels of control indeed work as a strainer, otherwise "if a pinpointed request is not possible, SWIFT would provide *all relevant* data - which could include names, addresses and personal identification numbers." (Lawton 2009) Then, the unmanageable amount of the required data would cut the real efficiency of the transfer as part of the preventive policy in anti-terrorist matters. These layers should see that the valuable information be extracted in due time, complying with the EU legal requirements and standards.

Even though after placing the servers under EU jurisdiction the Agreement does not fail to bind the US authorities to inform the EU about possible terrorist threats, the contribution of the US to the EU intelligence agencies may lessen. According to the former French investigating judge commissioned by the EU, Jean-Luis Brugière, before the restrictions the TFTP had generated considerable intelligence to the EU states. (JHA

[21] In the US legal system, the subpoena is a court summon. There are two types: the usual writ for the summoning of witnesses (ad testificandum) or the submission of evidence, as records or documents, before a court or other deliberative body (duces tecum). The administrative subpoena is a non-traditional tool of criminal investigation in the fields of secret service protection, health care fraud, child abuse, controlled substance cases, and Inspector General investigations. (Doyle 2005,2) This method helped bypassing traditional banking privacy protection rules.

[22] This kind of mechanism was used with the transfer of passenger data to the US.

Council, 2009:5) Now the restricting action of the EU may presumably cause a US reduction of intelligence towards the 'data provider'.

This causes many to strengthen their belief that in the field of counterterrorism the Agreement did not produce radical positive changes. German Justice Minister Sabine Leuthheusser-Schnarrenberger and the German Federal Police Agency consider that "granting intelligence agencies access to people's bank accounts doesn't provide any additional security, […] [because] "in terms of combating politically motivated crime, there is no technical requirement or operational interest in a systematic verification of the SWIFT database." (Spiegel online, www.spiegel.de/international/europe/0,1518,674789,00.html)

But what the Agreement actually realizes is that it questions whether there is perhaps also a necessity for a re-evaluation of the counterterrorism legislation to cope with the requested privacy needs while making sure that efficient measures of security can be taken. How can people feel free from fear of terrorist attacks without feeling their privacy is violated by the authorities responsible for security? On short term, this dilemma may restrain the transatlantic cooperation in the field of counterterrorism, which is so much needed to ensure global security, and brings to light that the response to the global threat is not yet global. It could not be at least as long as the discussion is still going on.

5. Conclusion

Even though the agreement is about the transmittal of financial data for the purpose of the counter terrorist fight, it actually directly concerns almost everybody, because it has multifarious legal, procedural, and security consequences and impacts on the privacy and the daily life of EU citizens. The debates around the SWIFT Agreement show that many questions still exist regarding the juridical and political construction of the EU data protection mechanism. They reveal the dilemma that the law makers and those enforcing the law are confronted with when ensuring a high level of security against terrorism while respecting the privacy rights of the citizens and coping with democratic principles. Moreover, they point out that terrorism and counterterrorism are still asymmetric, despite of the global cooperation in security matters. While everyone can fear the occurrence of

cross border threats, the policies to combat them cannot cross the borders of the legal and procedural practices.

In this sense, this interim Agreement is less a basic framework of personal data transfer and more a door for necessary comprehensive improvements in the legislation and practices in this field, to reduce the opposition of the two superpowers. Concerning the EU, it challenges the Commission, the Parliament and the Council to find solutions to the legal problems of the US-based regulation for data protection, and calls for a higher profile as unified actor in front of the unilateral US approach in international and security affairs. It proves that as long as the EU gives in to the US data protection standards and practices despite its clear communitarian laws, it accepts the US to act upon it for "improving regulatory standards"[23]. It induces that the EU accepts the US legislation to undermine the EU one, and the US interests to dominate the EU ones, fetching a blow right in the face of the Union's institutions and democracy. If the final SWIFT Agreement does not embrace this issue, the data protection differences will perhaps continue to dominate the transatlantic agenda.

A first step towards the solution of this problem supposes that the internal issues that concern the Union be clarified so that the EU may act less fractured in the foreign affairs with the US. In this respect, the EU disposes of 2 powerful instruments:

- the Treaty of Lisbon, for it binds the EU Council and Commission to involve the Parliament in all the phases of negotiations, which creates a different juridical context in both, inner and international affairs;
- the civil society, inasmuch as it exercises confidently its role as the second pillar within human security by asking how appropriate, proportional and effective such a data transmittal is as an instrument for identifying terrorist financing and capturing terrorists, and by pressuring the EU to be less submissive in issues like data protection practices.

[23] See the US National Strategy for Homeland Security.

Concerning the overseas partner, the debates encourage an adjustment of the US legislation – in a highly ideal case -, at least with respect to the Privacy Act, or the issue of addressing US courts by EU citizens inasmuch as data protection within the partnership is as important as the counterterrorist fight outside the western alliance. The first mentioned protects the citizens from the inside threats, whereas the second one protects them from the outside perils. This means that if counterterrorism focuses on people, its instruments (read protection in data transfers) should also have citizens as their highest command. As long as the parties infringe upon the fundamental rights and civil liberties of the other[24], they are impeded in their common defense policy and their reciprocal reliance is shadowed. Hence, as the conflicts created by the SWIFT Agreement show, it becomes binding that the partners agree upon common practices, based on highly commended principles, in order to be strong against others.

Even though one cannot really talk about its contribution to the fight against terrorism, an Agreement for financial data transfer has been necessary in the context of the SWIFT architectural changes. With all its advantages or breaches, it displays the common endeavors to master without delay asymmetric threats, as well as the EU efforts to turn the transatlantic partnership for combating terrorism as smooth as possible, trying for the time being to keep away from the public the sensitive subject regarding the US engagement with the EU security issues.

[24] Another example is the violation of the EU Directive 95/46/ED in the case of the transfer of the passenger data.

6. Bibliography

1. Brand, Constant, „Belgian PM: Data Transfer Broke Rules", in *The Washington Post*, 28.09.2006, El. Ed http://www.washingtonpost.com/wp-dyn/content/article/2006/09/28/AR2006092800585.html.

2. Dahl-Eriksen, „Tor: Human Security: A New Concept which Adds New Dimensions to Human Rights Discussions?", in *Human Security Journal* Volume 5, Winter 2007, El. Ed. Accessed 24.01.2010 http://www.peacecenter.sciences-po.fr/journal/issue5pdf/4.Eriksen.pdf.

3. Doyle, Charles, „Administrative Subpoenas and National Security Letters" in *Criminal and Foreign Intelligence Investigations*, Background and Proposed Adjustments. CRS Report for Congress. April 15, 2005, El. Ed. Accessed 22.01.2010 www.fas.org/sgp/crs/natsec/RL32880.pdf.

4. European Digital Rights: A new SWIFT agreement under negotiation between EU and USA. In: EDRi-gram Nr. 7.17. 09.09.2009. El. Ed. http://www.edri.org/edri-gram/number7.17/swift-european-parliament

5. *European Parliament: Resolution of 17 September 2009 on the envisaged international agreement to make available to the United States Treasury Department financial payment messaging data to prevent and combat terrorism and terrorist financing*, El. Ed. Accessed 24.01.2010 http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P7-TA-2009 -0016+0+DOC+XML+V0//EN

6. Financial Times Deutschland: „Datenstriptease erbost Wirtschaft", in *Financial Times Deutschland*. 30.11.2009 http://www.ftd.de/politik/deutschland/:swift-abkommen-datenstriptease-erbost-wirtschaft/50044462.html?page=2

7. Gellman, Barton/Blustein Paul/Linzer, Dafna: Bank Records Secretly Tapped.Administration Began Using Global Database Shortly After 2001 Attacks, in *Washington Post*, June 23, 2006. El. Ed. Accessed 22.01.2010 http://www.washingtonpost.com/wp-dyn/content/article/2006/06/23/AR2006062300167.html.

8. Justice and Home Affairs Council: BACKGROUND Note. Brussels, 27.11.2009, El Ed. Accessed 25.01.2010 http://blog.tech-and-law.com/2009/12/eu-transfer-of-financial-messages-data.html.

9. Kuner, Christopher, „Onward Transfers of Personal Data Under the U.S. Safe Harbor Framework", in *Privacy & Security Law*, 17.08.2009, El. Ed. Accessed 22.01.2010 http://www.hunton.com/files/tbl_s47Details/FileUpload265/2639/Kuner_Onward_Transfers_8.09.pdf.

10. Lawton, Michael, „EU approves data-sharing SWIFT agreement with US authorities", in *DW-World.de*. 30.11.2009, El. Ed. http://www.dw-world.de/dw/article/0,,4952263,00.html.

11. Levey, Stuart Levey, „Statement of Under Secretary Stuart Levey on the Terrorist Finance Tracking Program", 23.06.2006, in *The Press Room of the US Treasury Department*, El. Ed. http://www.treas.gov/press/releases/js4334.htm.

12. *Liberal International*, „The Oxford Manifesto of 1947", accessed 24.01.2010, www.liberal-international.org/editorial.asp?ia_id=535.

13. Lichtblau, Eric / Risen, James, „Bank Data Is Sifted by U.S. in Secret to Block Terror", in *The New York Times*, June 23, 2006, El. Ed. accessed 22.01.2010 http://www.nytimes.com/2006/06/23/washington/23intel.html?_r=1&hp&ex=1151121600&en=18f9ed2cf37511d5&ei=5094&partner=homepage.

14. López Aguilar, Juan Fernando, „SWIFT: European bank data transfers must comply with European standards, say MEPs", press release in *European Parliament site*. 03.09.2009, http://www.europarl.europa.eu/news/expert/infopress_page/019-60174-246-09-36-902-20090903ipr60173-03-09-2009-2009-false/default_en.htm.

15. Meyer, Josh / Miller, Greg, „U.S. Secretly Tracks Global Bank Data. The Treasury Dept. program, begun after the Sept. 11 attacks, attempts to monitor terrorist financing but raises privacy concerns", in *L.A. Times*, June 23, 2006, El. Ed. accessed 22.01.2010 http://articles.latimes.com/2006/jun/23/nation/na-swift23?pg=3.

16. Neely, Brett, „EU to share consumers' financial data with US", in *Deutsche Welle-World.de*, 13.11.2009, El. Ed. http://www.dw-world.de/dw/article/0,,4887522,00.html.

17. *Official Journal of the European Union*, „Processing of EU originating Personal Data by United States Treasury Department for Counter Terrorism Purposes – 'SWIFT'. Terrorist Finance Tracking Program – Representations of the United States Department of the Treasury (2007/C 166/09)", El Ed. accessed 24.01.2010 http://eur-lex.europa.eu/LexUriServ/site/en/oj/2007/c_166/c_16620070720en 00180025.pdf.

18. Schlamp, Hans-Jürgen, „Spying on Terrorist Cash Flows. EU to Allow US Access to Bank Transaction Data", in *Spiegel online International*, 27.11.2009 http://www.spiegel.de/international/europe/0,1518,663846,00.html.

19. Spiegel Online: Not So SWIFT. European Parliament to Reject Bank Data Agreement with US. 29.01.2010, El. Ed. Accessed 29.01.2010. http://www.spiegel.de/international/europe/0,1518,674789,00.html.

20. Spongenberg, Helena, „European Central Bank knew about US data access", in *EUobserver*, 29.06.2006, El. Ed. http://euobserver.com/9/21984.

21. UNDP, „New dimensions of human security", in *Human Development Report 1994*, Chpt. 2, El. Ed. accessed January 23, 2010. http://hdr.undp.org/en/reports/global/hdr1994/.

22. Vermeulen, Mathias, „EU approves data-sharing SWIFT agreement with US authorities", in *The Lift. Legal Issues in the Fight Against Terrorism*, 30.11.2009 http://legalift.wordpress.com/2009/11/30/eu-approves-data-sharing-swift-agreement-with-us-authorities/.

Ramona Ricarda POPA a absolvit în 2002 limba şi literatura germană şi engleză, la Universitatea Lucian Blaga din Sibiu. În anul 2003 a absolvit Academia Națională de Informații *„Mihai Viteazul"*, Bucureşti, iar în perioada 2007-2009 a participat la un curs de cercetare în domeniul păcii şi al conflictelor la Marburg (Germania). Până în prezent a realizat mai multe studii în domeniu, cu accent pe transformările sociale şi politice în perioadele de tranziție după conflicte sângeroase.