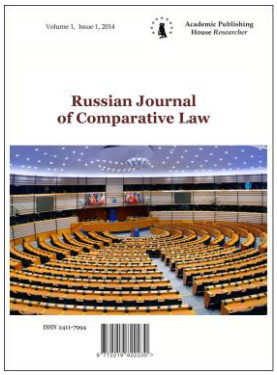
Published in the Russian Federation
Russian Journal of Comparative Law
Has been issued since 2014.
ISSN 2411-7994
E-ISSN 2413-7618
Vol. 7, Is. 1, pp. 4-10, 2016

DOI: 10.13187/rjcl.2016.7.4
http://ejournal41.com




Articles and Statements

UDC 343 (060.55), 341.01 (075)

# Counterterrorism and Data Transfers in International Trade

Frank Altemöller

Harz University of Applied Sciences, Germany
Friedrichstraße 57, Wernigerode, 38855
Doctor, Professor
E-mail: faltemoeller@hs-harz.de

**Abstract**

The ongoing developments show the growing threat posed by international terrorism – including to global trade. This article begins by outlining the initiatives being taken by the US and the European Union for trade security. Their success is, to a considerable extent, dependent on transfers of information between the participating states. But what is the effect of information sharing on the security of data provided by participating companies, for the privacy of citizens and, ultimately, for national sovereignty and the rule of law? This conflict, however, reaches even further. It goes beyond the "issue of security" and impacts deeply on the relationship between the US and the European Union. The article explores the role of public authorities of the US and the EU and the implementation of the relevant international laws and regulations.

**Keywords:** international law, international trade, the USA, the EU, customs and border protection, counterterrorism, data transfers.

## Introduction

The most recent attacks in Paris have shown unequivocally that the fight against terrorism will be one of the dominant policy issues of the future. The attack on New York's World Trade Center, carried out before our eyes on 11 September 2001, had already shown the potential dimensions of terrorism. Terror poses a threat, not only to civil society, but also to the world of international trade. Amongst customs and trade experts, a significantly increased awareness of risk has arisen: It was very quickly feared that international container traffic and seaports could come to the attention of terrorists. From low-security seaports, terrorists could extend their operations to reach international container traffic all over the world. Scenarios were developed, whereby terrorists in inadequately secured seaports could place bombs and other material for attacks into containers [1; 2; 3; 4]. In such scenarios, a potential threat of unprecedented proportions was quickly identified: In the "worst case" it was thought possible that, after a series of such attacks, no country could be sure that arriving containers would not contain even more bombs. In a subsequent panic, large parts of the container-transacted transport sector could, at least

temporarily, come to a standstill – with incalculable consequences, not only for individual ports and countries, but for the entire global economy [5; 6].

**Materials and methods**

The sources drawn on for the preparation of this article include legal, regulatory and policy documents of the US and the EU, the legislation of the European Court of Justice, as well as publications in journals and archive materials. The review is based on an analytical assessment and uses standard analytical methodologies, along with an examination of law from a comparative perspective. The author's arguments follow a chronological approach to examining the problems at hand. The historical and situational background is laid out and leads to an assessment of how international law standards in the US and the EU are implemented. The examination of comparative law further illustrates the differing views in the implementation standards of international law. The systematic approach used here makes a variety of disciplines (USA law, European law, commercial law etc.) accessible and open to comparison. And it ultimately illustrates that the present is determined by the past, just as present and past conditions will determine the future.

**Discussion**

*1. Security initiatives for global trade*

The USA, followed by other countries and the EU, responded with a range of initiatives [7; 8; 9; 10; 11; 12; 13]. These differ from each other in their specific protection objectives, and in their means of implementation. However, a significant, common characteristic is embodied in the fact that, until now, controls on container traffic have been carried out on imports, at the time of their arrival in the importing country. The new initiatives stipulate that the checks must now be displaced externally, to the actual dispatch location of the goods. The US "Customs and Border Protection ", for example, describes their CSI as follows: “The Container Security Initiative is a revolutionary program to extend our zone of security by pre-screening containers posing a potential security risk before they leave foreign ports for U.S. seaports [14]. Our goal is to process 85 percent of all containers headed for the United States through CSI ports by 2007“ [15]. The US security initiatives are discussed by, for example, see [16; 17; 18; 19; 20; 21].

The European concept of "Authorized Economic Operators" (AEO) is regulated in Art. 5a of the European Community Customs Code (CC). Important additional rules include Art. 14a to 14x of the Implementing Provisions the Customs Code (CC-IP). The concept of AEO consists of customs authorities identifying particularly reliable private operators and, following successful completion of an extensive examination procedure (certification), equipping them with specific trade-related privileges (so-called Authorised Economic Operator). This includes operational benefits – essentially a preferential and rapid settlement of customs procedures [22; 23; 24]. Taken together, these security concepts mean that high-risk cargo is identified before it even has a chance to reach the territory of the state which launched the initiative, (the principle of "Pushing Borders Out") [25; 26; 27]. Practical implementation, however, has shown the difficulty in identifying which risks are present at what stages of which supply chains. Therefore, the "visibility" of the supply chain is a critical factor in risk analysis. To determine risks and respond to them appropriately, governments and administrations need precise and up to the minute information about where any item of cargo is located in the supply chain – in other words, the ability to access this information in real time ("visibility on demand").

*2. Data transfers: a central element of the fight against terrorism*

These new security concepts throw up far-reaching questions: Not just regarding data protection, but extending particularly to the safeguarding of corporate data. Above all though, they raise issues of sovereignty under international law. The initiatives aimed at securing the supply chain break with hitherto common thinking, whereby the state’s security is ensured by those checkpoints that form the national borders. In contrast, it would now be increasingly advantageous to place the security controls ever further away.

To achieve this, intelligent systems collect the appropriate data and store it according to highly complex algorithms for specific, but also open-ended, and currently not yet foreseeable, purposes. This requires a high measure of collaboration among trading partners – primarily with

the countries from which the consignments most at issue will be sent. Regimes to secure the supply chain can thus be understood as real controls on virtual borders, i.e. borders that are projected out for the purpose of safeguarding the territory. For the initiatives to be practically implemented, it is therefore particularly important to have cooperation between the countries involved. To accomplish that, numerous agreements have been concluded to provide for mutual recognition and compliance with national and regional security regimes. They are of the utmost importance for international business practice:

For example, on 4 May 2012, the US and the EU reached an agreement for mutual recognition of their C-TPAT and AEO safety regimes. This came into effect on 31 January 2013. The agreement includes the comprehensive exchange of all relevant information amongst the participating countries. This mutual recognition is highly advantageous for the effected businesses: The US recognition of the European AEO means that the specific advantages of the C-TPAT are also conferred on business entities that don't have C-TPAT, but rather, have AEO certification. The same applies for US companies certified as C-TPAT, who are then brought within the scope of the AEO [28; 29; 30]. U.S. Customs and Border Protection has enhanced its partnership with import trade sectors, but challenges remain in verifying security practices [31].

The participating companies are very positive about their involvement in the international security programs, as it bestows on them clear and immediately tangible benefits. As a consequence, however, they must accept a diminished overview of what happens to their trade-related data once it has been submitted - in particular, what further dissemination is implied by international exchange and utilization. The possession of such data opens up an enormous strategic dimension. It is not surprising, therefore, that the USA in particularly, has been exposed to considerable criticism for its pioneering role. It has been argued that strategic considerations, rather than security, form the primary goal of the initiative, placing the far wider use of the collected data in the foreground [32].

This criticism, however, has not gained wide acceptance. Alan D. Bersin makes it unequivocally clear how important the unobstructed collection of data is, from the perspective of the United States. He quite stridently demands a change in thinking in the area of security, a change that fundamentally calls into question our current understanding of data protection [33, P. 3 et seq]. "The challenge of our times is that the future is not what it used to be" – with this quote from the poet Paul Valéry, Bersin asserts that anyone who is not able to adapt, is stuck in old ways of thinking and fails to recognize the challenge of our times. On a daily basis, the United States already exchanges billions of pieces of data with its trade partners - and in this area, "less is more" just does not apply. "Those who hoard information today, expecting their power to grow by forcing others to ask for it, soon find themselves isolated and, over time, ignored." [34, P. 3, 7]. Today it is critically important that all participating stakeholders contribute to risk reduction, through the exchange of information.

In an "anarchic world", without central global security structures, it resides in the sovereignty of individual states to launch initiatives directed towards this end [35; 36; 42]. However, approaches that remain limited to national initiatives can only inadequately fight the international terrorism phenomenon. And the compromised exchange of information allows even greater latitude for terrorists. Bersin says that information is power, and calls for a different perspective: "Old-fashioned, limited views of national interest, and reflexive notions of privacy and civil liberties, restrict willingness to share, and reinforce parochial and myopic concerns of long duration" [34, P. 3, 8]. He believes that a solution in the fight against terrorism will only come about through the free exchange of data and the consequent generation of actionable intelligence from that mass of information. And he asserts that data protection, as well as privacy, are assured. For only when signs of a "match" become evident, out of the multitude of anonymous algorithms, will the collected data be combined to produce recoverable information, and the previously existing privacy suspended.

This means that, in international trade, the state borders no longer serve directly as checkpoints for the guarantee of national security. In the future, it will be that exchange of information that determines where the "new frontiers" run.

*3. The conflict between security, data transfers and the rule of law*

"Border" traditionally signifies, principally, the opportunity to exercise control. But what opportunities for control are offered by the "new borders"? Fundamental questions come to mind: What about the protection of corporate data? What are the factors to be considered when balancing legitimate security concerns against other vital interests in need of protection? And above all: How can States ensure their citizens' fundamental constitutional freedoms in the face of "shifting traditional borders"? This development has long since become a reality and, as a result, the conditions affecting sovereignty and rule of law are changing. As an expression of their national sovereign rights, many states already regulate, to varying degrees, the collection and use of data within the national sphere. From Alan D. Bersin's point of view, the legitimization for exchanging data derives from a "bargaining process": „ ... the intersection between privacy protection and information sharing to enhance security in the global supply chain and global travel zones is crisp and sharp. One need not reconcile different visions, or points of departure concerning how to think about privacy, in order to arrive at a common position regarding what steps are required to protect personal data in a specific case. At end, some application of informed consent can account for a satisfactory outcome. In other words, entry and engagement in global travel or supply chain activity embodies a bargain between public authorities and private actors. The contours of the bargain regarding use and dissemination have long been settled once the threshold of entitlement to collection has been crossed" [37, P. 3, 15].

There can be no doubt that States, and the international community, must defend themselves against terrorism. The requirements of counterterrorism demand that data transfers are conducted on a far higher level. In critical situations, individual countries may not identify threats themselves, but are reliant on information from their exchange partners. Additionally, potential risks can be better identified when the respective knowledge of individual countries is summarized into an overall picture. This raises the question then, whether those involved in the negotiations on data transfers are fully aware of the associated consequences: Can the delegation of rights be justified in the name of collecting data for "open-ended" purposes? If the criteria under which the information is being collected remain unclear, then any assumptions as to how, and to what ends, it will be used later must be, by extension, vague and hypothetical. The European Court of Justice formulated principles for data transfers in the "Schrems" ruling: "Any such framework must therefore have sufficient limitations, safeguards and judicial control mechanisms in place to ensure the continued protection of the personal data of EU citizens including as regards possible access by public authorities for law enforcement and national security purposes" [38]. To this effect, on 2 February 2016, the EU Commission and the USA approved a new treaty for transatlantic data transfers (EU-US Privacy Shield). This set of rules is intended to address the Commission's heavily criticized and - by the ECJ - rejected "Safe Harbour" decision [39].

In the current debate, the tension between holding on to freedom or surrendering it through the disclosure of information, is becoming increasingly important. There is an argument that the liberal way of life needs to be actively defended to a far greater extent than used to be the case [40, P. 47]. The philosopher and writer Peter Sloterdijk, in particular, has proved quite polemical and provocative in drawing attention to this tension between enjoying freedom and defending it [41, P. 8]. Sloterdijk views Europe as being on the defensive. Till now, it has had little will, when required, to impose its interests by force. Rather, it has humbly depended on the quick acting and combat-ready United States to take on the task. In this relationship, the peaceable nature of one is made possible only by the boldness of the other. Sloterdijk points out that Europe's dependency on the defensive umbrella of the US has led to a significant sacrifice of European autonomy. This dependence affects virtually all policy areas, such as the "terms of trade" and many other economic sectors, the ceilings for emissions of exported diesel engines, the implementation of American skills standards or the screening of European data traffic, and even encompasses spying on European political leaders. Consequently, Sloterdijk calls for a stronger Europe and a Europe that speaks with one voice internationally. Only in this way will it be possible to regain lost "sovereignty", including that within the field of data control and usage.

The message, then, is that the international fight against terrorism, specifically in the collaboration between the US and Europe, needn't be conducted under asymmetric conditions, characterized by subservience and dependence. Recent developments have unequivocally demonstrated to Europe that its open society must be defended. And Europe well understands the

challenge. In meeting that challenge, Europe cannot defend itself from a position of dependency, but only from a position of strength, and this includes extensive cooperation with partners. The key now is how quickly Europe manages, under the preconditions of the considerable diversity and differing interests of the Member States, to formulate and assert its own way.

The dimensions are now shifting: It seems paradoxical that a state of freedom can only be achieved through a simultaneous defensive posture, even though that vigilance, as the example of data security shows, does not leave our civil rights untouched. Can enhanced security and greater political autonomy only be achieved by restricting freedom? This raises some far-reaching questions: Can enhanced security and broad political autonomy be achieved only by putting limits on our freedoms – and, if so, how much freedom must we surrender, in order to hold on to it at all?

**Results**

It is not just the civil society, but likewise the world of international trade, that finds itself exposed to the terrorist threat. To protect themselves, the US and the EU, along with other countries, have developed comprehensive regulatory regimes, such as C-TPAT and AEO. These approaches are based on separate national, or on European, approaches. The effective combating of terrorism, however, requires an international response. Because, at the international level, no regulatory framework, binding on all the States concerned, exists to protect international trade against terrorism, the States are obliged to cooperate with each other. This is achieved through comprehensive programs for the transfer of data.

**Conclusion**

The sharing of information between individual states is a central element in maintaining security in international trade. However, these data transfers profoundly impact on both the internal data security of corporations, as well as the privacy of citizens. It also raises fundamental questions about national sovereignty and the rule of law. Will safeguarding against terrorism mean a sacrifice of freedom? In the current debate, Europe is criticized for allowing its established values to be compromised. This comes about largely because Europe maintains its own “peaceable nature” by placing itself in a dependent relationship with the USA, a country which, by contrast, is self-assertive and ready to defend its interests and partners. Europe’s reliance on the United States goes to almost all policy areas, data security included. It is the position of this contribution, however, that the cooperation between the US and Europe needn’t be conducted under asymmetric conditions. By engaging in the defence against terrorism, whilst simultaneously pursuing greater security in data sharing, Europe can look after its own interests far more fully than it has done in the past.

**References:**

1. Mark Mazzetti and Scott Shane, Evidence Mounts for Taliban Role in Bomb Plot // N.Y. Times, May 2010.

2. Kenneth Chang, Explosive on Flight 253 is Among Most Powerful // N.Y. Times, December 2009.

3. Schweizer Ausgabe, Reaktion auf die Paketbomben aus dem Jemen // Neue Zürcher Zeitung, from 9 November 2010.

4. Hartmut Küchle, Seehäfen als neuralgische Zonen der kritischen Infrastruktur: Sicherheitstechnologische Lösungen und Arbeitsplätze am Beispiel des Hamburger Hafens. Bonn, 2008.

5. Frank Altemöller, Towards an International Regime of Supply-Chain-Security: An International Relations Perspektive // World Customs Journal. 2011. Vol. 5. № 2. September 2011. P 21-33.

6. Frank Altemöller. Risikomanagement im internationalen Handel: Wie schützt die Europäische Union den Containerverkehr gegen Terrorismus? // Niedostadek/Riedl/Stember (Eds.), Risikomanagement im öffentlichen Bereich, Schriftenreihe der Hochschule Harz “Forschungsbeiträge zum Public Management”. vol. 5. P. 375-400.

7. UN Security Council resolution No. 1373 from 28 September 2001 and also, No. 1456 from 20 January 2003 and No. 1624 from 14 September 2005, as well as the initiatives of the World Shipping Council.

8. In addition, the G8 adopted an initiative to reinforce security in the area of international transportation: The Cooperative G8 Action on Transport Security, 26 June 2002.

9. The World Customs Organization has developed an international framework (SAFE Framework) to secure and facilitate global trade, see: World Customs Organisation: WCO SAFE-Framework of Standards, Brussels, 2007.

10. Kunio M. Supply Chain Security: The Customs Community´s Response // World Customs Journal. 2007. Vol. 1. № 2. P. 51-60.

11. Ireland R. The WCO SAFE-Framework of Standards: Avoiding Excess in Global Supply Chain Security, WCI Research Paper № 3, Brussels November 2009.

12. Andrew Grainger, Supply Chain Security, Adding to a Complex Operational and Institutional Environment // World Customs Journal. Vol. 1. № 2. P. 17-29.

13. Organisation for Economic Co-operation and Development: Container transport security across modes, European Conference of Ministers of Transport. Paris, 2005.

14. U.S. Customs and Border Protection 2006, P. 2.

15. Maurice I. Supply Chain Security Programs and Border Administration // World Customs Journal. 2009. Vol. 3. № 2. P. 80-84.

16. Michael D. Laden, The Genesis of the US C-TPAT Program: Lessons Learned and Earned by the Government and Trade // World Customs Journal. 2007. Vol. 1. № 2. P. 75-80.

17. For a general analysis see, for example: Wieslaw Czyzowicz, Customs Policy and Customs Law in the Contemporary World Trade // Gwardzinska, Werner & Wierzbicki (Eds.), Customs Policy – Economics, Law and Practice, Szczecín, 2014. P. 18–52.

18. David Widdowson: The Changing Role of Customs: Evolution or Revolution? // World Customs Journal. 2007. Vol. 1. № 1. P. 31-37.

19. Widdowson, Holloway: Maritime Transport Security Regulation: Policies, Probabilities and Practicalities // World Customs Journal. 2009. Vol. 3. № 2. P. 17-42.

20. Heiner Heseler, New Strategies of port enterprises and their effects on the structures in the seaports // Rainer Dombois, Heiner Heseler (Ed.): Seaports in the Context of Globalization and Privatization, Maritime Studies. 2000. № 1. P. 9-27.

21. Michael Lux, A Layman´s Guide to Bringing Goods into the EU // Global Trade and Customs Journal. 2011. P. 121-129 and 131-142.

22. European Commission, Authorized Economic Operators 2006 und European Commission, Authorized Economic Operators 2007.

23. Hans-Michael Wolffgang, Talke Ovie, Emerging Issues in European Customs Law // World Customs Journal 2008. Vol. 2. № 1. P. 3, 12 et seq.

24. Maiya Polner: Compendium of Authorized Economic Operator (AEO) Programmes, WCO Research Paper № 8, Brussels July, 2010.

25. U.S. Customs and Border Protection, Container Security Initiative, 2006-2013 Strategic Plan, CBP Publication 0000-0703, Washington D.C., 2006.

26. U.S. Customs and Border Protection, Supply Chain Best Practices Catalogue, Customs-Trade Partnership Against Terrorism (C-TPAT), Washington D.C., 2006.

27. US-Department of Transportation Research and Innovative Technology Administration, America's Container Ports: Freight Hubs that Connect Our Nation to Global Markets, 2009.

28. European Commission, Directorate-General for Internal Policies: Customs Cooperation in the Area of Freedom, Security and Justice, Brussels 2011, Carsten Weerth, AEO Pragrammes Worldwide: From MRAs to a General AEO Agreement? // Global Trade and Customs Journal. 2015. Vol. 10. section 6. pp. 228-330.

29. Aigner, Susanne, Mutual Recognition of Authorized Economic Operators and Security Measures // World Customs Journal. 2010. Vol. 4. № 1. pp. 47-54.

30. Scholl, Susanne (Germany Trade and Investment), Gegenseitige Anerkennung von AEO und C-TPAT, Cologne 2009, as well as Government Accountability Office (GOA).

31. Report to Congressional Requestors, April 2008.

32. See also: Christopher Dallimore. Securing the Supply Chain: Does the Container Security Initiative Comply with WTO-Law?, PhD Thesis Münster University 2007.

33. For background, see: Alan D. Bersin (Assistant Secretary, US Department of Homeland Security), Lines and Flows: The Beginning and End of Borders // World Customs Journal. Special Compilation prepared for Inaugural Global Conference 21-23 May 2014.

34. Alan D. Bersin, Lines and Flows: The Beginning and End of Borders // World Customs Journal, Special Compilation prepared for Inaugural Global Conference 21-23 May 2014.

35. Continued in: Grillo, Cruise, D`Erman, Protecting our Ports, Domestic and International Politics of Containerized Freight Security. Farnham, 2010.

36. Oldrich Bures, EU Counterterrorism Policy, Farnham 2011 and: Robert Keohane: The Public Delegitimation of Terrorism and Coalitional Politics // Booth, Dunne (Eds.): Worlds in Collision: Terror and the Future of Global Order, London 2002.

37. Alan D. Bersin, Addendum I (Information sharing and personal data protection) to Lines and Flows: The Beginning and End of Borders // World Customs Journal, Special Compilation prepared for Inaugural Global Conference, 21-23 May 2014.

38. Communication from the Commission to the European Parliament and the Council, on the Transfer of Personal Data from the EU to the United States of America under Directive 95/46/EC following the Judgment by the Court of Justice in Case C-362/14 (Schrems), Brussels, 6 November 2015 COM(2015) 566 final. P. 3.

39. Commission Decision of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council, on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce (notified under document number C(2000) 2441) // OJ L 215. 25 August. 2000. P. 7-47.

40. Mark Lilla, Die stete Verbesserung der Illusionen, Lange wollte man in Frankreich nicht wahrhaben, dass die offene Gesellschaft verteidigt werden muss // Neue Zürcher Zeitung from 28 November 2015.

41. Peter Sloterdijk, Die Abhängigkeit des Friedfertigen vom Schlagfertigen // Neue Zürcher Zeitung, Meinung und Debatte, from 5 October 2015.

42. Andreas Wieland, Strategic Supply Chain Security // Journal of Homeland Security, March 2009.

УДК 343 (060.55), 341.01 (075)

**Контртерроризм и передача данных в международной торговле**

Франк Альтемёллер

Высшая школа прикладных наук, Гарц, Германия
Friedrichstraße 57, 38855 Wernigerode
Доктор наук, профессор
E-mail: faltemoeller@hs-harz.de

**Аннотация.** Происходящие события показывают растущую угрозу со стороны международного терроризма, в том числе в глобальной торговле. Статья начинается с изложения инициатив, предпринимаемых Соединенными Штатами и Европейским Союзом для безопасности торговли. Их успех в значительной степени зависит от передачи информации между странами-участницами. Но каково влияние обмена информацией о безопасности данных, предоставленных компаниями-участницами, на неприкосновенность частной жизни граждан и, в конечном счете, на национальный суверенитет и верховенство права? Этот конфликт выходит за рамки "вопрос безопасности" и глубоко воздействует на отношения между Соединенными Штатами и Европейским Союзом. В статье рассматривается роль органов государственной власти США и ЕС в осуществлении соответствующих международно-правовых норм.

**Ключевые слова:** международное право, международная торговля, США, ЕС, таможенная и пограничная охрана, борьба с терроризмом, передача данных.