Results of the workshop “Yes to Data Protection”

“Migrants and Consumer Protection in Digital Markets” - 13.06.2014

The second workshop of the project “Migrants and Consumer Protection in Digital Markets” was dedicated to the theme of data protection and was conducted in the rooms of the Consumer Advice Center on June 13th 2014. 26 participants took part in the event. Participants were 13 guests from the House of Representatives, the administrations of the federation and the state. Even six representatives from Russian immigrant organizations and associations such as the National Association of Displaced Persons, the Youth Migration Service (Schoeneberg branch), the International Confederation (Charlottenburg-Wilmersdorf branch office), the Schalach Youth and Family Center and Integration Center Box 66 attended the event,

Eva Bell, Chair of the Consumer Advice Center, opened with the workshop with the greeting in which she stressed the importance of data protection for people of a migrant background. She referred to a new draft law which will give Consumer Advice Centers the right to lead collective action against data protection breaches by Internet companies.

In her welcoming speech, Sabine Toepfer-Kataw, the Secretary of State for Consumer Protection, presented the results of the Berlin Consumer Monitor for 2013, which indicated enormous deficits in consumer education among people of Turkish and Russian origin. Many consumers are not sufficiently aware of the meaning of data protection. She claimed that a better awareness of data protection would have to be created for consumers in the use of sophisticated information and communication technologies. A preselection of user data in the Internet by companies such as Google enables the creation of consumer profiles and advertising aligned to this. Not only companies are interested in this data, but criminals too. Because of this, it is not only a matter of data protection, but also of prioritizing consumer protection. The Secretary of State concluded her welcoming address with the demand for the European Union to create strict standards and rules with regard to data protection and to make people aware of this matter.

Dr. Günter Hörmann, Director of the Consumer Advice Center of Hamburg, described the different field of action of the Consumer Advice Centers in the course of the last five decades, which have gradually adapted themselves to the needs of consumers. Hörmann emphasized the increasing significance of personal data in today’s information and communication society. The storage of telephone and internet data and the access to this without the knowledge of those concerned are liable to cause a feeling of constant surveillance of private life. Businesses are able to procure outstanding and monopolistic market positions through intelligent linking of data and thus to entice the consumer to use their services (examples are Google and Facebook). He referred to the decision of the European Court of Justice on the EU Guideline on Telecommunications Data Retention. The European Court of Justice rejected EU telecommunications data retention in April 2014, since it violates basic rights. Hörmann

stressed the importance of data protection not only for the protection of democracy but also for consumer protection as an indispensible requirement.

Dr. Çiçek Bacik, leader of the project “Migrants and Consumer Protection in Digital Markets”, underlined the particular role of migrants and the activities of the Berlin Consumer Advice Center for this target group. Alongside to advice in Turkish language by honorary lawyers, the Berlin Consumer Advice Center has now provided a Russian-speaking lawyer, who also holds monthly discussions on site in Marzahn and Lichtenberg in Russian and German. Futhermore, Bacik reported on the multiplier training under the “Mentor Training for Target Group-Oriented Consumer Protection“, which has existed since 2012.

Bacik emphasized that migrants represent a particularly vulnerable consumer group according to the 2013 Berlin Consumer Monitor and had a large need for information in the area of the internet and telecommunications. According to this, a majority (56% of Turks and 47% of Russians). Like a vast number of the German population, migrants also use the Internet to go shopping and to complete bank transactions. More than a third of Turkish and Russian-speaking consumers had already been confronted by problems with e-commerce and their smartphone bills were twice as high compared to the German population. Bacik underlined the particular meaning of the project for these reasons. While 85% of Germans in 2013 consciously decide which (personal) data may be accessed in the use of programs of apps, only 45% of people of Turkish origin and 37% of Russian speakers pay attention to he protection of their data, according to the Berlin Consumer Monitor.

Going into the project objectives in detail, Bacik explained various measures that are planned to educate Turkish and Russian-speaking consumers in the digital markets: Educating the target group about consumer rights, market and consultancy services in digital markets, investigation of the market situation in the telecommunications market through market checks and workshops, creating information in the area of telecommunications and the Internet, collecting complaints of the target groups and providing information on the competent use of telecommunication services, Internet and data protection. In the two planned market checks, the telephone rates for Turkey and Russia were in focus, whereby the examination and evaluation of prices, services and business practices of the telephone company is the main focus. A central project component is the subsequent provision of target group-oriented information about issues in the digital markets. Bacik mentioned that information for the target groups should be made available for the target groups in German as well as in Turkish or Russian summaries or info boxes. Finally, she reported on the result of the starting workshop.

Christian Daher, ICT Consultant from the Office of the Berlin Commissioner for Data Protection and Information Security, presented the basics on the safe use of WLAN and smartphones and told the participants about the data traces which consumers leave behind on the Internet. First of all, Dahler explained why it is important to always used encrypted WLANS when surfing the Internet. Since public buildings, cafes or shops do not always offer encrypted internet connections, these connections should be avoided. In particular, e-commerce services should be avoided with unencrypted Internet connections. Exceptions are secured VPN (Virtual

Private Network) and IPsec (Internet Protocol Security) connections. If possible, WPA and WPA2 (Wi-Fi Protected Access) encryptions should be used due to their security. Setting up a WPS (Wi-Fi Protected Setup) network may be convenient, but unsafe in some respects: The PINS could be stolen while an automatic Internet connection is set up 1-2 minutes after the computer is switched on.

Additional requirements for secure Internet surfing are using safer passwords which are difficult to guess and, if possible, not pre-defined for wireless networks which could be configured and managed if necessary with special software. Even deactivation of remote router configuration after setting up the network contributes to secure data transfer.

Dahler subsequently explained some basic security settings for smartphones, such as the use of a password to prevent unauthorized access to the device and the data stored on it, checking the download and use of free apps and checking the granting of access rights to data. Furthermore, one should be more careful with the localization function of some apps, since movement profiles for the users can be created, amongst other things. It is important to research information on unfamiliar apps. Checked apps in manufacturer stores are currently somewhat more secure. Apps for Android in particular are frequently not checked. Sensitive user data can be accessed by downloaded apps. It is often not clear who obtains the user data and what is done with it. For example, intercepted data could be used for advertising purposes while a game is being played, which is why it is better to turn off the WLAN when playing the game.

In the second part of his speech, Dahler explained which user data is transmitted when websites are used. By using data on the browser type, screen settings, operating system, information on the screen resolution and color depth, the type of device accessing the respective website can be determined, for example. The media have already reported on device-related consumer prices in connection with Apple devices.

A further possibility for using websites for the personalization and recognition of data are cookies. Cookies are small text files with information on visited websites, which have been stored on the users computer by these websites, in order to identify the user afterwards. Furthermore, the surfing behavior of individual users can be tracked via so-called tracking cookies from the search engines and re-sold to cooperating websites to create a targeted offer. Also, previous orders and earmarked products of the user are stored by online shops so tha they can offer the user additional relevant products. This type of data access can be minimized by turning off individual browser functions such as Flash and JavaScript and add-ons (small browser extensions) such as NoScript and AddBlock-Plus. Dahler emphasized the increased security while surfing in incognito mode and illustrated its setting in a browser.

Furthermore, Dahler informed the attendees about the right to right of informational law creation* in accordance with §§33-35 Federal Data Protection Law, under which the persons concerned demand both alerts and information on saved data and the correction, blocking and deletion of data. In conclusion, he reported on the so-called Robinson List

(www.robinsonliste.de), which promises protection from unsolicited commercial mail and telephone calls.

Dr. Kei Ishii and Polina Roggendorf from the project “Consumers Safe Online”, Technical University of Berlin, informed the participants on surfing the Internet safely. Using the example of a three-dimensional superstructure of a Russian-speaking news website, Roggendorf and Ishii illustrated the invisible interconnections of the Internet. They said that many processes on the Internet occur automatically and are invisible to the user. The aim of the invisible Internet is data collection. There are however applications which help to establish which businesses are tracking the surfing activity of the user. Using the example of the software Ghostery, Ishii showed how many and which businesses were observing the visit to a website which he had opened. That means that these businesses have access to user data and can use these together with the collaboration cookies for advertising purposes. The number of such websites which are operating invisibly can be over 100 for average surfing activity. The actual danger of data collection is not advertising, but the involuntary storage of data. The trend of the amalgamation of data which has been collected from different sources is constantly growing. The statistical recording and explanation of collected data is conducted for example by Piwik-Analytics[1]. Ishii went on to say that the operators of a website decide which data collection can be accessed by specialized companies on their websites. Through searches, site visits, Google, for example, learns certain user-specific information which are categorized within tenths of seconds via cookie-matching i.e. cookie comparison for the evaluation of surfing activity and are sold in the form of auctions by Google to advertising companies. In conclusion, Ishii shared important tips for securing your own data when surfing the Internet: Securing your computer by updating programs and anti-virus software and using safe passwords. Corresponding settings and functions of the browser are of enormous importance for the protection of data, such as the deletion of browsing history and cookies, as well as the use of browser plug-ins like Ghostery. Further assistance in securing your computer and personal data can be found by users in the project “Consumers Safe Online” (https://www.verbraucher-sicher-online.de/) and Internet Users have Rights (https://www.surfer-haben-rechte.de/). Furthermore, consumers should user their data as sparingly as possible and should not pass on any data.

Dr. Kei Ishii and Christian Dahler took part in the podium discussion. The discussion was presented by Ünal Zeran, the project leader from Hamburg. Dr. Turgut Altuğ (Bündnis 90/Die Grünen: The Greens), Speaker for Environmental and Consumer Protection in the Berlin House of Representatives, advocated that such educational events be carried out locally in migrant organizations, so that this information can also reach this target group. Heike Ansorena, Speaker for Commercial Consumer Protection, the Senate Department for Justice and Consumer Protection, asked with respect to the “right to be forgotten” (judgment of the ECJ) why Google requires a copy of the identity card in applications to delete personal data. Dahler replied that the demand for a copy of an identity card is not required by law, not even

[1] Piwik-Analytics is an alternative to Google Analytics. The open-source program collects and analyzes the data of website visitors. (Source: http://www.piwik-analytics.com/)

in the conclusion of mobile phone contracts, however, in reality, these guidelines are not adhered to. Google and other companies want to identify the applicant on the basis of an identity card. Furthermore, the removal of data by Google does not entail a complete deletion from the World Wide Web.

Conclusion

Migrants' lack of awareness of data protection, which already came to light in the Berlin Consumer Monitor in 2013, was confirmed both in the opening workshop of the project on 14 March 2014 and also at this second workshop. From the responses of the participants, it was clear how important specific recommendations are for action to protect your own data and for the security settings of your computer. The education of migrants on data protection and the strengthening of their media competence has to play an important role. Given that the Internet represents an indispensible medium in the everyday life of migrants and that they are confronted more severely by target-group specific pitfalls, the Berlin Consumer Advice Center is planning to issue a data protection information document for Russian and Turkish-speaking migrants in cooperation with the Berlin Data Protection Commissioner. The most important tips on data protection should be listed in this information. The target groups should be informed, why the security settings of a computer and a smartphone are important and why restraint in the submission of personal details is recommended for social networks and e-commerce. The contents should be available in the internet presence of the Consumer Advice Center. The project-specific interactive forum planned for November should take up at least one focus of data protection.

Feedback from workshop participants:

"Thank you for the great event!"

"I would like to thank you for inviting me to the workshop on data protection. It was very enriching."

"Thank you for the invitation! I will immediately alter the security measures on my computer!"