Issues related to the National Revenue Agency personal data leak.
Was the media and public institutions' reaction adequate?

Ten days after huge arrays of information were stolen from the National Revenue Agency (NRA), Veni Markovski, blogger and journalist, one of Internet pioneers in Bulgaria, comments on the failure in the information system of the agency. He mentions problems related to data misuse, media coverage and poor public institutions' handling of the situation.

First problem: the hacking of the databases. This is an extraordinary tax administration problem since the personal data of millions of Bulgarians was stolen.

Second problem: the reaction of NRA after the databases leak. It turns out that the only representative of the agency, who communicated with the media, was the PR expert. The situation was extremely tense and it was necessary someone from the agency management staff to explain to the public what exactly had happened and what measures would be undertaken.

Third problem: Stolen databases' usage. It became clear that individuals and at least one website – the Bulgarian alternative media *'Bivol'*, had published a form via which a reference could be made on the basis of the Personal Identification Number to check whether one's data had been stolen. Another Bulgarian IT expert also criticized the unofficial way through which personal data can be checked. He also argued that such formats are not trustworthy at all.

Such approach is rather risky since it reveals the creators of the forms either have the databases available or they have access to them in order to make the checks. Markovski stresses the fact that 'the usage of stolen information in any form, with any technical means is illegal and unjustified'. Stolen personal information is protected not only by the Bulgarian laws, but also by the EU. Personal data keeps its characteristics, no matter whether it is stolen or published.

Hacking can happen to any institution or company despite server protection measures. However, the usage of already stolen information, though meant "to make favor" to people who want to check whether leakage has happened to their data, is in practice not only a good motivation for another data stealing in the future but is also a reason for reflection about possible connections between the 'Bivol' media (dealing with investigative journalism) and the suspects.

The fourth problem, identified by Markovski, relates to the distribution of heaps of information in hackers' forums. *ZDnet* media representatives contacted a Bulgarian citizen with the nickname Instakilla who explained that he published the data after he saw a link to the files during the Bulgarian Television Nova streaming. When asked why he shared the databases of his fellow countrymen, having in mind the possibility for him to be arrested, he replied that he wasn't the

Project Number 762128
CALL: H2020-ICT-2016-2017
TOPIC: ICT-19-2017

original hacker and he did not feel 'responsible for anything'. "Will state institutions take the pains to find out who "Instakilla" is and will he be prosecuted?" asks Markovski. He also adds that as a consequence of Instakilla's behaviour, the database is very accessible for a download now. We have to recall that 'copying, holding and usage of stolen information is 'a breach of the law'.

The fifth problem according to Markovski is the Bulgarian television 'Nova'conduct and 'the fact that the media has aired unedited connection to the stolen databases, and later Instakilla has taken advantage of this'.

'I don't know if the Commission for Personal Data Protection will consider the issue on its own initiative', Markovski comments and underlines that journalists must be careful about the way they distribute information.

The sixth problem is that the authorities and the media raise preliminary accusations despite the presumption of innocence. 'Until now what we know from the prosecution office and from the media is that there are three persons with pressed charges. The company's name where they work was also announced and photos documenting the confiscation of their office equipment were distributed. However, there is no evidence that these people are the hackers, who penetrated the servers of NAP', Markovski concludes.

Compiled by Media 21 Foundation from https://blog.veni.com/?p=5589