Mg. iur. Martins Birks
Sworn Attorney at Law
Postgraduate Studies in ICT,
IP & Media Law
Katholieke Universiteit Leuven

"THE NEO CASE – CRIME COMMITTED OR WELL ORGANIZED POLITICALLY MOTIVATED PUNISHMENT?"

CASE ANALYSIS

Table of Content

1. Introduction to the Case

The climate, as such, was ripe for a public outcry. Latvia was hit hard by the 2008 global financial crisis. Unemployment rates had increased from 9 per cent to 23 per cent in just a year, and were the highest in the European Union. The economist Paul Krugman noted in December of 2010, "The most acute problems are on Europe's periphery, where many smaller economies are experiencing crises strongly reminiscent of past crises in Latin America and Asia: Latvia is the new Argentina; Ukraine is the new Indonesia."[1]

"There is very little trust in Latvia's institutions right now, so anyone who can expose the system is going to be a hero," said the Latvian political commentator Juris Kaza[2] in the spring of 2010. The summary below describes the particulars of the so-called "Neo case" [3], where a citizen, calling himself "Neo", uncovered a loophole in the governments State Revenue Service website and, as a result, was able to expose the inflated salaries of the state-run company bosses and high ranking public service officials[4].

The case revolves around the individual named Ilmars Poikans, whose actions caught the attention of the Latvian State Police. Ilmars Poikans is a Latvian artificial intelligence researcher, who reportedly admitted to being the cyber activist known as Neo (hereinafter – Neo). Using the pseudonym of Neo and portraying himself to be a member of the cyber-activist group called the 4ATA (Fourth Reawakening People's Army), Neo discovered and then exposed a serious security flaw in the State Revenue Service Electronic Declaration System (EDS). Through his Twitter account (twitter.com/neo4ATA), and files uploaded via Media fire server on February 14, 2010, he revealed that unauthorized persons could take advantage of a flaw in the Electronic Declaration System software developed by stock company Dati Exigen to access the tax records of any taxpayer in Latvia.[5] Because of this flaw, any internet user, without authorization, could download any EDS documents by simply typing in

[1] http://www.nytimes.com/2008/12/15/opinion/15krugman.html
[2] http://freespeechlatvia.blogspot.com/
[3] http://www.movements.org/case-study/entry/a-web-savvy-latvian-uncovers-and-spotlights-public-corruption/
[4] http://www.movements.org/case-study/entry/a-web-savvy-latvian-uncovers-and-spotlights-public-corruption/
[5] http://en.rsf.org/latvia-judicial-authorities-urged-to-end-25-08-2010,38199.html.

the web-address and document number, hence putting at risk everyone's private information such as taxes paid, persons codes, and other sensitive data.[6]

Neo uncovered the flaw by chance, while putting the finishing touches on his own tax returns using the State Revenue Service's online system[7]. Ilmars, being a self-professed "IT guy" and a researcher at the Institute of Mathematics and Computer Science at the University of Latvia, also has his own IT business, which specializes in start-ups. Before adopting the Neo moniker he was not a political activist, he was mainly just passively watching what was going on in politics and had written an article expressing his views about referendums, and the possibility and conditions under which people could revoke the power of the parliament through self-initiated action. In spotting information that was in the public domain, but that no one had noticed, and deciding to do something with that data, he moved away from being a passive watcher of Latvian politics and ended up transforming himself into an activist and public informant.

Through this security loophole, Neo obtained 7.4 million classified files, including VAT receipts and income tax returns from the State Revenue Service public website. The tax data downloaded by Neo involved high ranking government officials and revealed that the much talked about austerity measures and mandatory salary cuts in the government sector were not, in fact, affecting the highest paid officials. In the following days, Neo proceeded by re-formulating the data so that it would be easy to read and understand what the information meant, and published it by sending out links to his own presentations of the data via Twitter.[8]

Neo published the salaries of various government agencies, at first withholding their identities, but later identifying the employees by name. He uncovered to the public the treasure troves politicians were harboring, padded by excessive bonuses, instead of proof of the salary cuts they had promised the public they would take. He published the salary of Latvian police chiefs and urged regular officers to analyze the data supplied by him and to determine from it if the salary

[6] http://www.tiesibsargs.lv/lat/tiesibsargs/jaunumi/?doc=264.
[7] http://www.movements.org/case-study/entry/a-web-savvy-latvian-uncovers-and-spotlights-public-corruption/
[8] http://www.movements.org/case-study/entry/a-web-savvy-latvian-uncovers-and-spotlights-public-corruption/

reform they had been subjected to was indeed fair[9]. Another leaked document showed the salaries of bank managers at the bank bailed out by the government – Parex Banka. The document revealed that the many promises the bank had made to the government to cut salaries, was in fact not kept. Neo also released data showing that the CEO of Riga's heating company, Aris Zigurs, paid himself a 16,000 lat ($32,000) bonus last year—a hefty sum for a city-owned utility, especially at a time when many municipal workers had their salaries slashed. Zigurs confirmed to the Latvian media that the data was indeed accurate.[10]

In publishing this information, Neo urged for a national reawakening in regards to the government lies and corruption at the highest level and was hailed a hero by the disgruntled Latvians.[11] Neo was depicted as the Robin Hood of hackers in much of the media coverage of what he did, but what he had done was actually not hacking at all. The information that he supposedly "uncovered" was already out there, just that nobody until then had published it in an understandable format. It was by turning the data into a digestible format that Neo was able to make an impact. As he himself has said, all he did was downloaded most of the data that was in the system, process it, and produce reports for different companies where people could see salaries of employees, for each company, month by month. Then those files were uploaded to file-hosting services, and links to those files were published on Twitter. After this, portals and newspapers began to publish the data showing who earned what.

While it was helpful, and perhaps necessary, for the media to have discovered the link on Twitter and republish the data in a medium with a broader audience, the problem was that these media reports "weren't pressing government institutions or even asking tough questions—no one was attempting to hold these politicians accountable"[12]. As a result, there was far less public outrage than one might have expected. As Neo has said "if there had been real outrage" ignited by the press, "there would have been bigger consequences....People are so passive in Latvia....My guess is

[9] http://www.technologyreview.com/wire/24651/page1/
[10] http://www.movements.org/case-study/entry/a-web-savvy-latvian-uncovers-and-spotlights-public-corruption/
[11] http://en.rsf.org/latvia-judicial-authorities-urged-to-end-25-08-2010,38199.html.
[12] http://www.movements.org/case-study/entry/a-web-savvy-latvian-uncovers-and-spotlights-public-corruption/

that in Greece or France there would be big demonstrations requiring some measurable change but not in Latvia...protest is not part of the culture in Latvia." [13]

The hole in the State Revenue Service's online system was soon closed, and the widespread protest that Neo had expected never came about. However, there were consequences to his actions. In the late evening of May 12, 2010, Ilmars Poikans was arrested at his workplace, the University of Latvia's Computer Science department. The Latvian police detained Mr Poikans on suspicion that he was Neo and had illegally obtained and leaked public sector salary statistics, violating data protection legislation.[14]

Upon analysis of the sequence of events and the actions taken by Latvian state officials, it seems that the Latvian authorities have taken a very strange and one-sided approach to this case. Although Poikans continue to be the target of judicial proceedings, the general problem of the software developed by DATI Exigen and the people responsible for the flaws have been largely left alone. The investigation of the State Revenue personnel responsible for the flaw in the system, and into the stock company DATI Exigen, a privately owned company, has been terminated. The only measure taken was to deduct 20 per cent from the salaries of three tax office employees for one month as a disciplinary measure.[15]

There has been no follow-up discussion about how such a security breach could have happened, to what extent is the government responsible for guarding personal data entrusted to the State Revenue Service, or the changes that need to be implemented to prevent future incidents. However, the individuals who made public to their fellow-citizens the dangers to their privacy, and reported on a matter of public interest, are being prosecuted (Ilze Nagla a well known Latvian journalist, who first reported on the data leak from the State Revenue EDS system, is also involved in judicial proceedings). The authorities seem to be showing a marked preference for media silence in a case involving key elements of state responsibility.

Another interesting aspect of the case is the fact that none of the information made public has been disputed by the national authorities, leading to the conclusion that the published information has been absolutely true. In further analyzing this case,

[13] http://www.movements.org/case-study/entry/a-web-savvy-latvian-uncovers-and-spotlights-public-corruption/
[14] http://freespeechlatvia.blogspot.com/2010/05/latvian-tv-investigative-journalists.html.
[15] http://en.rsf.org/latvia-judicial-authorities-urged-to-end-25-08-2010,38199.html.

the Author would like to investigate to what extent, if any, does content of leaked information bear significance on the substance of the case. As the information made public by Neo relates to the public sector and tax payers money, especially in the context of government reduced spending, does the public have a right to know and does judicial precedent term this type of information to be of public interest?

Neo quickly earned, what the BBC called "cult status,"[16] aggravating authorities and energizing citizens to call for increased government accountability in the Baltic State. However, more than a year later, the unemployment rate remains as high as ever in Latvia, and in the latest Corruption Perception Index, released on October 26, 2010, Latvia has earned a score of 4.3 and dropped to a ranking of 59th in the 2010 Corruption Perceptions Index released by the Berlin-based Transparency International. In 2009, Latvia received a score of 4.5 and ranked 56th.[17]

Has anyone been held accountable for the information Neo exposed? Can we expect Neo, even as the government threatens him with jail time, to find the time to develop a more sustainable mechanism for allowing citizens to monitor information that should be in the public domain? The authorities who originally detained Neo for alleged illegal access to the tax records have only released him on probation pending another trial - will he be detained again? The criminal investigation is in progress since 2010. What Neo's efforts have shown, is that sometimes important steps towards calls for transparency do not have to incorporate complicated tactics and hacking, but can be as simple as putting a spotlight on information already available.

As described elsewhere[18], there have been some positive outcomes: A law has been passed in May that requires state institutions to publish its data in much the same manner as Neo originally did—according to company and with each salary displayed on a monthly basis. With his actions, Neo had pointed out the lack of transparency in the system, and at least with the current version of the law there is more information available than has been before.

[16] http://news.bbc.co.uk/2/hi/technology/8533641.stm
[17] http://latviansonline.com/news/article/7083/
[18] http://www.movements.org/case-study/entry/a-web-savvy-latvian-uncovers-and-spotlights-public-corruption/

2. Particulars of the Case

In order to move forward with this project, the author would like to explain how the State Revenue Electronic Declaration System (EDS) works and then outline the chronology of events.

In Latvia, it is possible to submit electronically declarations, reports and tax calculations to the State Revenue Service (SRS) through the internet by using Electronic Declaration System (EDS). The SRS EDS system was envisioned as a convenient and easy to use program, available to all taxpayers - legal entities and natural entities. Currently via EDS it is possible to submit 95 per cent of all the reports and declarations foreseen in normative acts, including all the most popular and most often used reports and declarations.

On February 4, 2010, the Managing Director of the State Revenue Service submitted to the State Police Central Criminal Police Department Economic section (hereinafter – VP GKPP EPP) a complaint stating that in the time frame between October 29, 2001 and February 3, 2010 there had been unsanctioned downloading of documents from the Electronic Declaration System. The documents, saved in XML format, contained information on personal and corporate data. As a result of these downloads, an unauthorized third party had come into possession of sensitive material, and violated the Law on State Information Systems and Personal Data Physical Protection Law.

As it was attested by an SRS employee, on 06.07.2009., Ilmars Poikans attempted to request a non-existent EDS document and on 24.08.2009. downloaded a document not applicable to himself from the EDS. After these instances, several other downloads and later massive EDS XML downloads of documents happened.

Ilmars Poikans has stated that the data possessed by SRS EDS system was, in fact, publically available to anyone without any authorization, one simply had to open the internet address: https://www2.vid.gov.lv/eds/Pages/GetDuf.aspx?id=. The data downloaded from SRS EDS system was downloaded using a program that anyone could download for Windows-systems and Apple Macintosh systems, (also several Linux-based and other UNIX-standard operating systems), called - **cURL**, which is a computer software project providing a library and command-line tool for transferring data using various protocols.

The downloaded documents were numbered in sequence, and the processed data, or more specifically links to the processed data, were published on http://www.twitter.com/neo4ata. In the salary lists made public, the names of the employees were replaced with Person Nr. X, except in the case of the Republic of Latvia Ministry employees and Saeima (Parliament) employees. In these lists the name and last name of the specific person receiving the salary was disclosed.

Example of downloaded and published information:

Employer	**Name**	**Period**	**Amount of salary**	**Average salary in month**
State or regional institution or company	Person X,	Year, month	XXX LVL	XXX LVL
Ministry or Parliament	Name of the person	Year, month	XXX LVL	XXX LVL

3. Chronology of the Case Materials

1. On February 4, 2010 the Managing Director of the State Revenue Service submitted to the State Police Central Criminal Police Department Economic section (hereinafter – VP GKPP EPP) a complaint stating that in the time frame between October 29, 2001 and February 3, 2010 there had been unsanctioned downloading of documents from the Electronic Declaration System. As a result of these downloads, an unauthorized third party had come into possession of sensitive materials protected by state legislation on data protection. On February 10, 2010, the VP GKPP EPP launched criminal process Nr. 11816003310 into the potential unsanctioned breach of State Revenue Service Electronic Declaration System.[19]

2. On May 11, 2010 the State Police Central Criminal Police Department Economic Section investigator Jeļena Fedeņeva made the decision to issue a search warrant for the work place of Ilmars Poikans room **xxx**, with the goal of finding and removing the hard drives with the illegally downloaded documents from the SRS ED systems data base XML, with programs designed to obtain and share such data, as well as other objects that would relate to the case of the violations committed.

3. On May 11, 2010 the State Police Central Criminal Police Department Economic Section investigator Jeļena Fedeņeva made the decision to issue a search warrant for the residence of Ilmars Poikans **xxx**, with the goal of finding and removing the hard drives with the illegally downloaded documents from the SRS ED systems data base XML, with programs designed to obtain and share such data, as well as other objects that would relate to the case of the violations committed.

4. On May 11, 2010 the State Police Central Criminal Police Department Economic Section investigator Jeļena Fedeņeva made the decision to issue a search warrant for the internet service space used by Ilmars Poikans **xxx**, with the goal of finding and removing the hard drives with the illegally downloaded documents from the SRS ED systems data base XML, with programs designed to obtain and share

[19] http://www.tiesibsargs.lv/lat/tiesibsargs/jaunumi/?doc=264.

such data, as well as other objects that would relate to the case of the violations committed.

5. On May 11, 2010 the State Police Central Criminal Police Department Economic Section investigator Jeļena Fedeņeva made the decision to issue a search warrant for the places frequented by Ilmars Poikans **xxx**, with the goal of finding and removing the hard drives with the illegally downloaded documents from the SRS ED systems data base XML, with programs designed to obtain and share such data, as well as other objects that would relate to the case of the violations committed.

6. On May 11, 2010 the State Police Central Criminal Police Department at the University of Latvia 'LU Mathematics and Information Institute' detained Ilmars Poikans on the grounds of preventing him from hampering the investigation, continuing criminal activity, or covering up the crime. During the questioning Ilmars Poikans admitted that in the time frame from 29.10.2009 to 04.02.1010 he downloaded massive amounts of data from the SRS ED system on legal entities and individual persons. He admitted to compiling the data, and distributing the data using a specialized program. He also admitted to isolated attempts at downloading data on July 1, 2009, and in Augusts and September. I.Poikans stated that all the data downloaded from ED system was processed and saved on the external hard drive "Buffalo", for security reasons the data was encrypted, and always in I. Poikans possession. Detention protocol was drafted on the grounds of the above mentioned actions.

7. On May 11, 2010 State Police Central Criminal Police Department Economic Section conducted a search at Ilmars Poikans place of employment – University of Latvia agency "LU Mathematics and Information Institute" with the goal of finding and removing information storage units and documents related to the SRS EDS data base. A Search protocol was drafted on the ground of the above mentioned activities.

8. On May 11, 2010 State Police Central Criminal Police Department Economic Section conducted a search at Ilmars Poikans place of residence with the goal of

finding and removing information storage units and documents related to the SRS EDS data base. A Search protocol was drafted on the ground of the above mentioned activities.

9. On May 11, 2010 State Police Central Criminal Police Department Economic Section conducted a search at Ilmars Poikans father's, Anatolijs Poikans, place of residence with the goal of finding and removing information storage units and documents related to the SRS EDS data base. A Search protocol was drafted on the ground of the above mentioned activities.

10. On May 11, 2010 State Police Central Criminal Police Department Economic Section conducted a search of Ilmars Poikans. A Search protocol was drafted.

11. On May 13, 2010 the State Police Central Criminal Police Department Economic Section investigator Jelena Fedeņeva made the decision to declare the person of interest a suspect, therefore declaring Ilmars Poikans as a suspect in criminal activity, in accordance with Criminal Law Section 244 Paragraph 2 and Section 145 Paragraph 1:

    - The Criminal Law Section 244 Paragraph 2 stipulates that for a person who commits the illegal manufacture, adaptation for utilization, sale, distribution or storage of such devices (also software), which are intended for the influencing of automated data processing system resources for purposes of committing a criminal offence, if substantial harm is caused thereby, the applicable punishment is deprivation of liberty for a term not exceeding four years or community service, or a fine not exceeding one hundred and fifty times the minimum monthly wage.

    - The Criminal Law Section 145 Paragraph 1 states that for illegal activities involving personal data of a natural person, if it has caused substantial harm, the applicable punishment is deprivation of liberty for a term not exceeding two years, or custodial arrest, or community service, or a fine not exceeding one hundred times the minimum monthly wage.

12. On May 13, 2010 the State Police Central Criminal Police Department Economic Section investigator Jeļena Fedeņeva made the decision to appropriate security measures in the Ilmars Poikans case, as a result the suspect Ilmars Poikans had to reside in a specific place of residence and was forbidden to leave the country.

13. On May 18, 2010 Ilmars Poikans turned to the Republic of Latvia State Police Central Criminal Police Department Economic Section investigator Jeļena Fedeņeva with a request to stop the criminal process against Ilmars Poikans because the committed offences do not constitute a criminal offence.

14. On May 19, 2010 Ilmars Poikans turned to the Finance and Economic Crimes Investigation Prosecutor I.Minajeva with a complaint that the search conducted at Ilmars Poikans place of employment, declared residence, and internet service space, and frequented places was unlawful, and asking to investigate the facts in the complaint and to evaluate the actions of J.Fedeneva making unwarranted decisions about conducting searches, their urgency, and making decisions in the order specified by the Office of the Prosecutor Law by a person directing the proceedings.

15. On May 19, 2010 Ilmars Poikans turned to the Finance and Economic Crimes Investigation Prosecutor I.Minajeva with a complaint that the detention of Ilmars Poikans was unjustified and hence unlawful – the investigator J.Fedeneva in authorizing I.Poikans detention violated I.Poikans basic rights and freedoms, because as stated in the Constitution Section 94 „everyone has a right to liberty and security of person. No one may be deprived or have their liberty restricted otherwise than in accordance with law". The complaint asked to check and evaluate J.Fedenevas actions, and if the decisions were made in accordance with the order specified by the Office of the Prosecutor Law by a person directing the proceedings in relation to I.Poikans basic rights.

16. On May 19, 2010 Ilmars Poikans turned to the Finance and Economic Crimes Investigation Prosecutor, Prosecutor General V.Ulmja with a complaint that the search conducted at Ilmars Poikans place of employment, declared residence, and internet service space, and frequented places was unlawful, and asking to

investigate the supervising public prosecutors I.Minajevas actions, in approving the search warrant, not establishing its justification and legality, as well as failing to establish its urgency as specified by the Office of the Prosecutor Law by a person directing the proceedings.

17. On May 25, 2010 Ilmars Poikans turned to the Republic of Latvia State Revenue Service with the request:
    - To send to expertise or audit the material copies, that were preformed after the SRS ED system was established to be susceptible to XML data downloads of physical and individual data, that happened from October 29, 2009 to February 4, 2010;
    - To inform if with the above mentioned downloads the data stored in the automated system was in any way affected, and if so to inform in what way was the data affected and to send the appropriate copies;
    - To inform if with the mentioned download SRS has suffered any damages, and if so then to inform about the exact damages caused, and how they are evaluated by the SRS and to send the appropriate copies;
    - To inform of the results of SRS conducted service tests and/or disciplinary investigations and measures taken in accordance with Personal Data Physical Protection Law and the names of the individuals involved.

18. On May 26, 2010 the Chief Prosecutor of the Finance and Economic Crimes Investigation unit V.Ulmis, after investigating I.Poikans complaint about the supervising prosecutor I.Minajevas actions, replied that Prosecutor I.Minajeva was justified in approving the search order.

19. On May 26, 2010 the State Police Central Criminal Police Department Economic Section investigator Jeļena Fedeņeva made the decision to reject fully the request made by I.Poikans to stop the criminal process, and informed I.Poikans of the decision on May 28, 2010.

20. On May 29, 2010 Finance and Economic Crimes Investigation unit Prosecutor I.Minajeva, after evaluating the complaint about J.Fedenevas actions, stated that in conducting the process of investigation J.Fedeneva had not violated I.Poikans

rights to freedom and violated his rights, and has acted in accordance with the processes specified in the Criminal Law.

21. On June 10, 2010 the State Revenue Service declined Ilmars Poikans request for the specified information.

22. On June 3, 2010 Ilmārs Poikāns turned to the Republic of Latvia State Data Inspection with the request:
    - To inform if the State Data Inspection after the incident with the State Revenue Service XML data about natural and legal entity downloads which had taken place from October 29, 2009 to February 4, 2010, and the said material publication, had received complaints from natural or legal entities about the possible violation of data protection, and if such complains have been made, then to inform what have been their evaluation results, and within the appropriate limits to add the necessary documentation copies;
    - To inform if the State Data Inspection after the mentioned download and material publication has conducted a review upon its own initiative, and if such a review has taken place, then to please inform of the results, and within the appropriate limits to add the necessary documentation copies.

23. On June 21, 2010 State Data Inspection informed Ilmars Poikans, that it had received only two complaints from individuals about the SRS EDS document download, and that the complaints were sent for evaluation to the corresponding institutions.

24. On June 4, 2010 Ilmārs Poikāns turned to the Finance and Economic Crimes Investigation unit Prosecutor I.Minajeva with a complaint asking to overturn the State Police Central Criminal Police Department Economic Section investigator Jeļena Fedeņeva decision on May 26, 2010 to deny the request of Ilmars Poikans to stop the criminal process against Ilmars Poikans because the committed offence do not constitute a criminal offence.

25. On June 4, 2010 Ilmārs Poikāns turned to the Chief Prosecutor of the Finance and Economic Crimes Investigation unit V.Ulmis with a complaint in which he asked to evaluate J.Fedenevas actions within the criminal process, and evaluate the supervising prosecutors I.Minajevas insufficient actions in controlling the actions of the person directing the proceedings, and failing to react within the process established by the Office of the Prosecutor Law to the violation of I.Poikans basic rights.

26. On June 17, 2010 Finance and Economic Crimes Investigation unit Prosecutor I.Minajeva, after evaluating Ilmars Poikans complaint, replied that there was no basis for overturning the State Police Central Criminal Police Department Economic Section investigator Jeļena Fedeņeva decision on May 26, 2010 to deny the request of Ilmars Poikans to stop the criminal process against him because of lack of criminal content to the offense committed.

27. On June 28, 2010 Chief Prosecutor of the Finance and Economic Crimes Investigation unit V.Ulmis, after evaluating the complaint of I.Poikans about the supervising prosecutors I.Minajevas actions, considered the complaint of Ilmars Poikans as unfounded.

28. On July 9, 2010 Ilmārs Poikāns turned to the State Police Central Criminal Police Department Economic Section investigator Jeļena Fedeņeva, and asked to be informed if within the scope of the criminal investigation Ilmars Poikans communication means had been controlled, and if so then withink what time period had the tapping of communication means happened and who of the investigative judges had made the authorizing decision.

29. On July 21, 2010 State Police Central Criminal Police Department Economic Section investigator Jeļena Fedeņeva informed Ilmars Poikans that the requested documents and information about tapping of communications means was classified investigation material, and therefore, this information could not be made public.

30. On August 19, 2010 Ilmārs Poikāns turned to Chief Prosecutor of the Finance and Economic Crimes Investigation unit V.Ulmis with a complaint about the actions of the supervising prosecutor. In the complaint I.Poikans requests an evaluation of I.Minajevas actions in not establishing the content of I.Poikans complaint against J.Fedenevas actions, as well as not giving J.Fedenava instructions about terminating the criminal process against I.Poikans because the committed offenses do not constitute a criminal offense, as well as to delegate to the supervising prosecutor to sufficiently monitor the actions of the person directing the proceedings and substantiate future decisions.

31. On September 27, 2010 the Chief Prosecutor of the Organized Crime and Other Specialized Crime Division A. Cernisevs, in replying to the August 19, 2010 complaint of Ilmars Poikans, denied the requests made.

32. On July 21, 2011 the State Police Central Criminal Police Department Economic Section investigator Jeļena Fedeņeva having reviewed the criminal process Nr.11816003310 material, concludes that:

1. *the facts and circumstances of the case, that have been established during the criminal process, suggest that in order to download the data from the Electronic Declaration System, I.Poikans used the operating systems "Linux" standard program "curl", which is a publically available facilitator for data downloading, and hence, is not an illegal automated data processing system resource for the purpose of influencing automated data processing system resources. Therefore, it does not meet the criteria set forth in the applied section of the law, thus, the criminal process in accordance with Criminal Law Section 244, Paragraph 2, is to be terminated due to lack of evidence that a crime has been committed.*

2. *Criminal Law Section 241, Paragraph 1, stipulates as punishable actions that are arbitrary (without the relevant permission or utilizing the rights granted to another person) accessing an automated data processing system or a part thereof, if breaching of data processing protective systems is associated therewith or if substantial harm is caused thereby. Paragraph 3 of the section, dealing with*

persons who commit the acts provided for in Paragraph 1 of the Section against the State information system, envisions a heightened level of responsibility.

It has been determined, that on June 1, 2007 the Electronic Declaration System, in accordance with 02.05.2002. Law on State Information Systems Section 13, and 02.08.2005 Cabinet of Ministers Regulation Nr. 527 "State Information System Registration Requirements", has been registered in the State Information System register as a state information system. In accordance with Law on State Information Systems Section 12, the Electronic Declaration System data base is State property, and its owner is the State Revenue Service. Further, the Electronic Declaration System is classifiable as a critical state information system in accordance with Law on State Information Systems, Section 16, Paragraph 1, as it contains data on information pertinent to revenue collection, necessary for the State to perform important economic, political and security functions, as well as data that, if damaged or destroyed, would hinder the ability to meet fundamental human rights. In the course of the investigation, the evidence gathered suggests that I.Poikans on-line, arbitrarily, without the relevant permission, accessed information resources stored within the state information system and threatened their confidentiality, integrity or availability. I.Poikans did not have legally granted user access, therefore, all his further actions and their consequences can not be considered as legal. As a result of his unsanctioned access, I.Poikans with intent, in an extended period of time, downloaded from the Electronic Declaration System 7,453,411 unique documents of legal entities or physical individuals not belonging to him. I.Poikans actions resulted in a serious threat to the State apparatus, the security of the society, to the general order, the existence of the competitive market was threatened, as were individual's basic human rights to privacy and data protection. Therefore, I.Poikans actions, in arbitrary access to the state information system and causing substantial harm, can be viewed as illegal activity preformed in accordance with actions stipulated in Criminal Law Section 241, Paragraph 3.

3. *Criminal Law Section 200, Paragraph 2, foresees criminal responsibility for unauthorized acquisition of economic, scientific technical, or other information in which there are no commercial secrets for use or disclosure by himself or herself*

or another person or commits unauthorized disclosure of such information to another person for the same purpose, as well as well as commits unauthorized disclosure of inside information of the financial instrument market.

It has been established, that the unlawfully downloaded State Revenue Service files contained merchant information that, according to the Commercial Law Section 19, Law on Accounting Section 4, and Freedom of Information Law Section 7, can be deemed as commercial secrets. Therefore, by acquiring documents that contain commercial secrets for his own use, I.Poikans has committed a crime according to the Criminal Law Section 200, Paragraph 2.

Based on the above and in accordance with the Criminal Procedure Law Latvia Section 29 Paragraph 2.1, Section 392[1], Section 377. Paragraph 1.2, Section 68 Paragraph 1.2, the State Police Central Criminal Police Department Economic Section investigator Jelena Fedeneva decided to

1. **Terminate the criminal process Nr.11816003310 according to Criminal Law Section 244, Paragraph 2, due to the lack of evidence that a crime has been committed.**
2. **Terminate the criminal process according to the Criminal Law Section 244, Paragraph 2, due to lack of harm done as a result of the actions.**
3. **Annul the 13.05.2010 decision declaring Ilmars Poikans as a suspect in criminal activity in accordance to Section 244, Paragraph 2.**
4. **Continue the investigation in accordance with Criminal Law Section 143, Paragraph 1.**
5. **Further to classify in the criminal process Nr.11816003310, the crime to be investigated according to the Criminal Law Section 241, Paragraph 3 and Section 200, Paragraph 2.**

33. On July 21, 2011 the State Police Central Criminal Police Department Economic Section investigator Jelena Fedeneva made the decision to declare the person of

interest a suspect, therefore declaring Ilmars Poikans as a suspect in criminal activity, in accordance with:

1. Criminal Law Section 241 Paragraph 3, which stipulates that for a person who commits arbitrary (without the relevant permission or utilizing the rights granted to another person) accessing an automated data processing system or a part thereof, if breaching of data processing protective systems is associated therewith or if substantial harm is caused thereby, if they are directed against the State information system, the applicable punishment is deprivation of liberty for a term not exceeding eight years or a fine not exceeding one hundred and eighty times the minimum monthly wage.

2. Section 145 Paragraph 1 which stipulates that for illegal activities involving personal data of a natural person, if it has caused substantial harm, the applicable punishment is deprivation of liberty for a term not exceeding two years, or custodial arrest, or community service, or a fine not exceeding one hundred times the minimum monthly wage.

3. Section 200 Paragraph 2 which stipulate that for a person who commits unauthorized acquisition of economic, scientific technical, or other information in which there are commercial secrets, for use or disclosure by himself or herself or another person, or commits unauthorized disclosure of such information to another person for the same purpose, as well as commits unauthorized disclosure of inside information of the financial instrument market, the applicable punishment is deprivation of liberty for a term not exceeding five years or custodial arrest, or community service, or a fine not exceeding one hundred times the minimum monthly wage.

4. Possible Punishment in Accordance with The Criminal Law Section 241 Paragraph 3

On July 21, 2011, the State Police Central Criminal Police Department Economic Section investigator Jelena Fedeneva made the decision to declare the person of interest a suspect, therefore declaring Ilmars Poikans as a suspect in criminal activity, in accordance with Criminal Law Section 241 Paragraph 3.

The Criminal Law Section 241 Paragraph 3 stipulates that that for a person who commits arbitrary (without the relevant permission or utilizing the rights granted to another person) accessing an automated data processing system or a part thereof, if breaching of data processing protective systems is associated therewith or if substantial harm is caused thereby, if they are directed against the State information system, the applicable punishment is deprivation of liberty for a term not exceeding eight years or a fine not exceeding one hundred and eighty times the minimum monthly wage.

In accordance with The Criminal Law commentary,[20] the criminal act (serious crime) endangers personal rights to exercise the access rights to resources contained within the system. The subject of analysis is a telecommunication system – structural information technology or the content of a data base. The action under objective evaluation is the unsanctioned access to automated data processing systems or its parts. With unsanctioned, in this case, it is understood as access to automated data processing systems without the proper authorization or using some other persons sanctioned rights.

According to the commentary, the offence to be punishable in accordance with Sections 241, Paragraph 1, depend on the following conditions:

1) that they relate to breaching of data processing protective systems and

2) as a result of the offence, substantial harm is caused (material in substance).

With automated data system's protective system, it is understood as special logistic protection system that the guilty person overcomes by either **breaking or bypassing with special methods.**

In accordance with the „The Criminal Law Implementation and Realization Order "[21] Section 23, Paragraph 1, one is responsible in accordance with the Criminal Law for the offence committed, if as a result of the offence committed not only is

[20] „Krimināllikuma zinātniski praktiskais komentārs 3" Sevišķā daļa, Zinātniskais redaktors Dr.Habil. Jur. Prof. U.Krastiņš, Firma „AFS", Rīga, 2007

[21] The Criminal Law Implementation and Realization Order, 15.10.1998.

substantial material loss (material loss which at the time of the incident is more than five times the minimal monthly wage of the Republic of Latvia), but other interests or rights protected by law are also threatened or if such threat is substantial.

As it has been analyzed in specialist judicial literature, Criminal Law Section 241, foresees arbitrary access to automated data processing systems as threatening the information access rights, as only the owner of the information system or the rightfully appointed manager is legally allowed to set the access rights to the information system, therefore arbitrary access will always violate the interests of the previously mentioned persons[22] In the first and sectond Paragraph the actions are classified as less serious crimes, in the third Paragraphy as serious crime.

The Section if applicable to arbitrary (without the relevant permission or utilizing the rights granted to another person) accessing of an automated data processing system or a part thereof if, 1) breaching of data processing protective systems is associated therewith and 2) if substantial harm (material in substance) is caused thereby.

Therefore, in evaluating the objective actions there has to be – access to the automated data processing system that is arbitrary, hence, without the relevant permission or utilizing the rights granted to another person.

Access - user right to access the computer network, specific computer network servers, or directories and files, that are created in computer network servers, and is granted by an administrator, overseer, or a system manager, determining the specific extent of rights to use the existing system resources[23]. Therefore, an authorized user is any person who through law, contract or other judicial means is legally allowed the rights to use, oversee, control, test, and use for academic research or in any other legal way employ information system resources.

If the specific user has not received such access rights to lawfully use the system resource, it is valid to term access arbitrary to the automated data processing system if 1) the system has a specified legal access procedure and 2) access is not preformed physically on location but on-line.[24] Access is considered arbitrary also in instances where the person will utilize the rights granted to another person in accessing an automated data processing system.

---

[22] Ķinis U. Kibemoziegumi. - Rīga: Biznesa augstskola Turība, 2007, 110.lpp.
[23] Piekļuve - http://www. termini. lv/index.php?term =access%20rights&lang=EN&terms =acces sbility.
[24] Ibidem, page 133.

As already been mentioned, one of the prerequisites to determine criminal responsibility in arbitrary access has to do with data processing protective system's breach by either bypassing or breaking protective measures. With the logical protection methods, it is understood as information and program protection means that facilitate the information system user identity and access rights validation, protects information from intentional or unintentional modification (damage) or deletion (destruction).[25] The actions will not constitute a crime if the person will have arbitrarily accessed the automated data processing system without the system having been secured with the respective protection measures.

Compulsory to establishing the seriousness of the offence are the consequence of the action is determining if there has been **substantial harm**. Therefore, it has to be established that the arbitrary access to the automated data processing system has resulted in significant material loss, or threat to other spheres and interests protected by the law, or that the threat to other legally protected interests and rights is significant.

In accordance with „The Criminal Law Implementation and Realization Order" Section 23, Paragraph 2, significant material loss is definable as loss which at the time of the incident is more than five times the minimal monthly wage of the Republic of Latvia. In the particular application, according to U.Kin's option, the loss could be calculated by taking into account the following 1) losses stemming from system downtime; 2) expenditure stemming from damaged information recovery or replacement; 3) expenditures stemming from new program resource installation, that foresees system security function renewal; 4) expenditure stemming from correcting the system user access rights; 5) lost profit, if the system provides information services for a nominal fee.[26] Presumably, such a calculation method in determining the extent of material loss, could also be used in determining if the crime committed has caused substantial harm in measuring the material loss.

In determining if other rights and interests protected under the law have come under threat, and if the threat can be classified as significant, U.Kinis, in using the experience of two other countries USA and Germany, recommends dividing all state systems into four groups: systems with a low risk of threat, systems with limited

[25] State Infomation Systems Law, May 22, 2002.
[26] Ķinis U. Kibemoziegumi. - Rīga: Biznesa augstskola Turība, 2007, 170.lpp.

degree of threat, systems with high degree of threat, and systems with very high social threat level.[27]

On the subjective level, Criminal Law Section 241 envisions that the offence committed is an intentional crime, because the person intentionally, without the relevant permission, or utilizing the rights granted to another person, accesses automated data processing system or a part thereof, breaching data processing protective systems, and in wishing to cause significant damage, knowingly allowing the possibility that damage might result or in being indifferent to the effects of the offence.

In accordance with the Law on State Information Systems Section 1 explanation, the State information system is a structured aggregate of information technology and databases, the use of which ensures the proposal, creation, compilation, accumulation, processing, utilization and destruction of information. State information systems are registered in the State Information System Register[28].

What Ilmars Poikans did was change the Uniform Resource Locator (URL), in the concrete case the web address of the web application, which is in fact just a website, by altering a number in the address on his own computer.

When one visits a website a document (the website) is downloaded from a computer system (the web server) and placed temporary on the user's computer memory, and displayed in the user's web browser. In choosing to request a website from the web server, one can enters a web address (URL) in the web browser address bar, one can click a link which leads to a URL coded in the (website) document where the link is found, or this is automatically downloaded by another document using a URL coded in the document.

One of the web addresses of this particular web application includes a number that is an identifier of the document requested by the user. By altering this number (referring to Mr. Poikans own ED document) and requesting the document from the web server with this new URL, Mr. Poikans downloaded another document from the webserver: someone else's ED document.

Mr. Poikans automated this process of altering the URL and visiting the website (downloading it to his computer) by having a script (a small computer

[27] Ibidem, Pages 166-168.
[28] State Information register, http://www.visr.eps.gov.lv/visr.

program he made) iterate over the document number and downloading the documents (using the cURL program) with all the different URL's to a specific place on his computer memory (instead of a temporary cache, where the web browser stores the documents to show).

This lead to Mr. Poikans having ED documents of several Latvian (legal/natural) persons on his computer memory (in this case, a removable hard drive). He processed the data (manually or automatically) in these documents to be more easily understood by others and published this information again on the internet.

By downloading a document from the system with another identifier (the number in the URL) than the identifier of his own ED document, he did not "influence" the "automated data processing system resources" as it was stipulated and mentioned in applicable Section 244 Paragraph 2 of The Criminal Law in another way than any other user using the system. By downloading his own document, or any other documents, he did not alter/destroy data on the system. Possibly, in a computer file on the web server system a log is written of all downloaded documents (who downloaded what and when). This file would thus be "influenced" by Mr. Poikans downloading documents, but it is influenced in the same way if any other Latvian would download his own ED documents.

Moreover, as there were not any technological or after effect in the Electronic Declaration System and it did not show any problems in its functions, none of the activities can be classified as preformed with the purpose to create such problems. Or what is called a "Denial of Service Attack" or "DoS Attack". Therefore, there is no "purpose of committing a criminal offence" involved in the actions preformed. As "Denial of Service" (the web server infrastructure stops working because it cannot cope with a massive load of requests) did not occur, Ilmars Poikans conduct could not be classified under the Section 241, Paragraph 3, of The Criminal Law, because in his conduct there was not breach of data processing protective systems, and Ilmars Poikans conduct did not result in any harm caused. Therefore, the offence cannot be classified according to the Criminal Law referenced section, as there has been no substantial harm caused and the details of the offence do not match the specified circumstances in the law.

Taking into account the formal specifications of Section 241 applied to the Ilmars Poikans case, the specifications state that the committed crime is considered as having taken place, or finished, in the instance that the actions specified in the

paragraph are committed. However, Ilmars Poikans did not start or finish any of the activities mentioned in this Paragraph, and the intention of Ilmars Poikans was not to commit a crime. The criminal proceedings should be terminated because the actions of Ilmars Poikans, as stated in The Criminal Law Section 241, Paragraph 3, do not correspond to the actual actions preformed.

5. Possible Punishment in Accordance with The Criminal Law Section 145 Paragraph 1

On May 13, 2010 the State Police Central Criminal Police Department Economic Section investigator Jeļena Fedeņeva made the decision to declare the

person of interest a suspect. Ilmars Poikans was declared a suspect in criminal activity in accordance with Criminal Law Section 145 Paragraph 1.

The Criminal Law Section 145 Paragraph 1, states that for illegal activities involving personal data of a natural person, if it has caused substantial harm, the applicable punishment is deprivation of liberty for a term not exceeding two years, or custodial arrest, or community service, or a fine not exceeding one hundred times the minimum monthly wage.

In order to establish if the activities committed by Ilmars Poikans could be classified as punishable in accordance with The Criminal Law Section 145 Paragraph 1, it is necessary to constitute whether the publication of salaries of state authorities could be acknowledged as illegal activities involving personal data.

In accordance with Latvian Personal Data Protection Law Section2 Article 3[29] personal data is any information related to an identified or unidentifiable natural person. For Ilmars Poikans to be punishable under The Criminal Law Section 145 Paragraph 2, a breach of Latvian Personal Data Protection Law has to be established.

As it is stated Latvian Personal Data Protection Law Section 3 Paragraph 3, the law is not intended to apply to the information systems made by natural persons in which personal data are processed for personal or household and family purposes and in which the personal data collected are not disclosed to other persons.

The documents published by Ilmars Poikans, or the list of the salaries, can be further divided into two categories:

1. The lists where the names of the employees were replaced with Person Nr. 1, Person Nr.2, Person Nr.3 etc, hence protecting their identity;
2. And the lists containing the salaries and corresponding names of the employees of the Ministries and Parliament of Latvia.

In relation to the first lists, where the names were not identified, in accordance with Latvian Personal Data Protection Law, the simple act of publishing the lists of salaries without revealing names can not be acknowledged as publishing personal data. The lists did not identify concrete person to whom the published date relates to.

[29] Personal Data Protection Law, from 23.03.2000.;

In relation to the second list, the Law on Prevention of Conflict of Interest in Activities of Public Officials in Latvia[30] becomes applicable. The stated purpose of the Law on Prevention of Conflict of Interest in Activities of Public Officials, Section 2, is to ensure that the actions of public officials are in the public interest, prevent the influence of a personal or financial interest of any public official, his or her relatives or counterparties upon the actions of the public official, to promote openness regarding the actions of the public officials and their liability to the public, as well as public confidence regarding the actions of public officials. Section 4 identifies a list of Public Officials to whom this law is applicable, which includes members of the Parliament and Ministers.

In accordance with Law on Prevention of Conflict of Interest in Activities of Public Officials in Latvia Section 23 Paragraph 1, a public official has a duty to submit the following declarations within the time period specified and in accordance with the procedures specified:

1. a declaration to be submitted upon assuming the office;
2. a declaration for the current year;
3. a declaration to be submitted upon ending the duties of office; and
4. a declaration to be submitted after the performance of duties of office has been terminated.

Public officials, with the exception of the public officials referred to in Paragraphs 3 and 4, are required to submit declarations to the State Revenue Service in electronic format by using the electronic declaration system of the State Revenue Service (Section 23 Paragraph 2).

(Public officials working in the State security authorities, with the exception of the Director of the Constitution Protection Bureau, are required to submit declarations to the Director of the Constitution Protection Bureau (Section 23 Paragraph 3).

The head of the Prevention and Combating of Corruption Bureau is required to submit his or her declaration to the Prime Minister or his or her authorised person (Section 23 Paragraph 4).

In accordance with Law on Prevention of Conflict of Interest in Activities of Public Officials in Latvia Section 26 Paragraph 1, in order to ensure the protection of personal data, the declarations shall contain a part that is publicly accessible and a

[30] Law on Prevention of Conflict of Interest in Activities of Public Officials in Latvia, from 25.04.2002;

part that is not publicly accessible. The public official, or the head of the authority which verifies declarations in accordance with the Law, as well as the head of the State or self-government authority who has received copies of the relevant declarations shall be responsible for ensuring public access.

The part of declaration that is publicly accessible is all the information included in the declaration, except the information that is specified in Paragraph 4 (Section 26 Paragraph 2).

Within the meaning of this Law, public access is the right of employees of the mass media and other persons to become acquainted with the declarations of any public official, as well as to publish the information included therein (Section 26 Paragraph 3).

The part of a declaration that is not publicly accessible is the place of residence and personal identification number of the public official, his or her relatives and other persons specified in the declaration, as well as counterparties, including debtors and creditors specified in the declaration (Section 26 Paragraph 4).

Only such public officials and authorities which examine the declarations in accordance with this Law, as well as in cases determined in the Law – prosecutors and investigative institutions or State security authorities may become acquainted with the information in the part of the declaration that is not publicly accessible (Section 26 Paragraph 5).

The data to be published indicated in the declarations of the President, members of the *Saeima*, Prime Minister, Deputy Prime Ministers, Ministers, Ministers for Special Assignments, Parliamentary Secretaries and councilors of city councils shall be published electronically no later than within one month, but the data to be published indicated in the declarations of other public officials not later than within three months after the submission thereof to the State Revenue Service (Section 26 Paragraph 6).

The significance of this law to the Ilmars Poikans case is that, even though Ilmars Poikans published the salaries of the concrete persons of public interest and named them, the information he published was stipulated by The Law on Prevention of Conflict of Interest in Activities of Public Officials in Latvia to be public and accessible in accordance with the Latvian legislation.

Further, the cited Criminal Law Section 145, applies only in cases where there has been illegal activity involving personal data of natural persons and also substantial

harms has been caused. In accordance with the law „The Criminal Law Implementation and Realization Order "[31] Section 23, Paragraph 1, one is responsible in accordance with the Criminal Law for the offence committed, if as a result of the offence committed not only is substantial material loss (material loss which at the time of the incident is more than five times the minimal monthly wage of the Republic of Latvia), but other interests or rights protected by law are also threatened or if such threat is substantial.

Taking into account the formal specifications of Section 145 applied to the Ilmars Poikans case, the specifications state that the committed crime is considered as having taken place, or finished, in the instance that the actions specified in the paragraph are committed. However, Ilmars Poikans did not start or finish any of the activities mentioned in this Paragraph, and the intention of Ilmars Poikans was not to commit a crime. The criminal proceedings should be terminated because the actions of Ilmars Poikans, as stated in The Criminal Law Section 145, Paragraph 1, do not correspond to the actual actions preformed and the consequences of the action, required for criminal liability, have not taken place.

6. Possible Punishment in Accordance with The Criminal Law Section 200 Paragraph 2

On May 13, 2010 the State Police Central Criminal Police Department Economic Section investigator Jelena Fedeneva made the decision to declare the person of interest a suspect. Ilmars Poikans was declared a suspect in criminal activity in accordance with Criminal Law Section 200, Paragraph 2.

[31] The Criminal Law Implementation and Realization Order, 15.10.1998.

Criminal Law Section 200, Paragraph 2, stipulate that for a person who commits unauthorized acquisition of economic, scientific technical, or other information in which there are commercial secrets, for use or disclosure by himself or herself or another person, or commits unauthorized disclosure of such information to another person for the same purpose, as well as commits unauthorized disclosure of inside information of the financial instrument market, the applicable punishment is deprivation of liberty for a term not exceeding five years or custodial arrest, or community service, or a fine not exceeding one hundred times the minimum monthly wage.

As it has bene analyzed in judicial literature[32], the criminal offence addressed in the Section of the Criminal Law is to be considered a less serious crime. The target of the crime – economic interests of the business and economic activity sphere, the object of the crime – information (economic, scientific technical or other information), that is secret or contains commercial secrets of a business or organization. The object of the crime can also be financial instrument and insider market information.

The section specifies criminal liability for commercial secret obtainment or disclosure (commercial secret – information that has commercial value if it remains a secret for unauthorized persons).

As a commercial secret can, for example, be accounting information. According to the October 14, 1992 Law on Accounting Section 4, "For accounting purposes, information and data, which in accordance with the existing regulatory enactments is required to be included in the reports of an undertaking, shall not be deemed to be commercial secrets.

All other accounting information of an undertaking shall be deemed to be commercial secrets and shall be accessible only for audits, to the tax administration for verification of the correctness of tax calculations, and to other State institutions in cases provided for by legislative enactments"[33].

The Criminal Law, Section 200 specification in „The Criminal Law Implementation and Realization Order "[34] in describing the offence committed that

[32] „Krimināltiesības. Sevišķā daļa. Trešais papildinātais izdevums", Zinātniskais redaktors Prof. U.Krastiņš, Tiesu namu aģentūra, Rīga, 2009

[33] Latvijas Republikas Saeimas un Ministru kabineta Ziņotājs, 1992, Nr.44; 1995, Nr.3, 23; 1996, Nr.24; 1999, Nr.15; 2000, Nr.10; 2003, Nr.12; 2004, Nr.6; 2006, Nr.10.

[34] The Criminal Law Implementation and Realization Order, 15.10.1998.

would qualify for criminal liability under the specific section requires the following actions: that the information is obtained in an illegal manner (through blackmail, bribery, intimidation, etc.), that the information is disclosed (communicated in any way to at least one person). The crime is considered as having taken place when the above mentioned actions have concluded.

The offence outlined in the third paragraph of the Section, stealing of the information (thievery, committing a robbery, fraud, misappropriation) can be committed through action. However, if information documents have been obtained through thievery, criminal liability is appropriated according to the Section 200 and Section 274, that deals with material crime. If in the process of stealing the information violence or threat has taken place, then criminal liability takes into account offence committed against a persons life and health. Criminal liability will also happen if the information is disclosed, without permission, by an employee of the business or organization (Criminal Law Section 195 and Section 200).

The offence, in Section 200, can only be committed with clear intent. The intent has to be on acquiring the unauthorized information for use or disclosure by himself or herself or another person, or disclosure to another person for the same purpose. The Section views as potential perpetrator of the crime a person, that according to law is responsible for safekeeping of the information (someone who, according rules and regulations, is responsible), and any physical individual who has reached the age of fourteen (company employee or any other individual). A State official cannot be criminally liable under this Section, as criminal liability for such an act is governed by Criminal Law Section 317, 318, or 329 upon applicable basis.

I.Poikans did not acquired the data in an illegal manner, and that there was no intent on behalf of I.Poikans to use the information on his own behalf or for use by another person, and as already mentioned the information was disclosed only partially and in an acceptable way. Further, all the acquired information was saved in a hard-drive that at all times was in the possession of I.Poikans. Therefore, the actions of I.Poikans can not be classified under Criminal Law Section 200, Paragraph 2.

7. Publishing Personal Data as Form of Freedom of Expression

In order to establish whether the activities of Ilmars Poikans can be punishable by The Criminal Law Section 145 Paragraph 2, it is not only necessary to constitute if the activities performed by Ilmars Poikans are admissible as criminal, but also to establish if such interference in his case from the governing authorities is not a violation of his freedom of expression rights. In other words, it is important to establish if Ilmars Poikans had the right to impart the information on the public and if his actions were "necessary in a democratic society".

Ilmars Poikans published the salaries of state authorities in Latvia, and urged the public to analyze whether the salary reforms and austerity cuts they had been subjected to where also applicable to the authorities. The document revealed that the many promises made to cut salaries, was in fact not kept in the higher echelons of the state. In publishing this information, he urged for a national reawakening in regards to the government lies and corruption at the highest level. Therefore, it can be construed that the activities performed by Ilmars Poikans were in the name of public interests. The basic presumption being that the public has a right to know where their tax payer money is being spent.

The right to freedom of expression and information is not only stated in the Constitution of the Republic of Latvia Section 100, which states that everyone has the right to freedom of expression, which includes the right to freely receive, keep and distribute information and to express his or her views, and prohibit censorship. But is also guaranteed by Article 10 of the European Convention for the Protection of Human Rights and Fundamental Freedoms in all 47 member states of the Council of Europe, including Latvia.

Article 10 – Freedom of expression stipulates:

1. **Everyone has the right to freedom of expression. This right shall include freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers. This article shall not prevent States from requiring the licensing of broadcasting, television or cinema enterprises.**

2. **The exercise of these freedoms, since it carries with it duties and responsibilities, may be subject to such formalities, conditions, restrictions or penalties as are prescribed by law and are necessary in a democratic society, in the interests of national security, territorial integrity or public safety, for the prevention of disorder or crime, for the protection of health or morals, for the protection of the reputation or rights of others, for preventing the disclosure of information received in confidence, or for maintaining the authority and impartiality of the judiciary.**

As previously analyzed,[35] Article 10 (1) stipulates the principle of the right to freedom of expression, while Article 10 (2), by referring to "duties and responsibilities" that go together with the exercise of this freedom, opens the possibility for public authorities to interfere in this freedom by way of formalities, conditions, restrictions and even penalties. Yet, the main characteristic of Article 10 (2) is precisely that, by imposing the so-called 'triple test', it substantially reduces the possibility of interference with the right to receive and impart information and ideas. Interferences by public authorities are only allowed under the strict conditions that any restriction or sanction must be "prescribed by law" must have a "legitimate aim" and finally and most decisively, must be "necessary in a democratic society".

Article 10 of the Convention, as interpreted by the European Court, has manifestly contributed to the guarantee of a higher level of protection of freedom of expression in addition to the constitutional protection in the member states and complementary to other international treaties protecting freedom of expression and information[36]

As it was stated by D.Vorhoof[37], Article 10 has to be interpreted from a perspective of a high level of protection of freedom of expression and information, even if expressed opinions or information are harmful to the State or some groups, enterprises, organizations or public figures. As set forth in Article 10, freedom of expression is subject to exceptions, which must, however, be construed strictly. The need for any restrictions must be established convincingly, precisely because freedom of expression is considered essential for the functioning of a democratic society[38].

---

[35] FREEDOM OF EXPRESSION UNDER THE EUROPEAN HUMAN RIGHTS SYSTEM FROM SUNDAY TIMES (N° 1) V. U.K. (1979) TO HACHETTE FILIPACCHI ASSOCIÉS ("ICI PARIS") V. FRANCE (2009) Prof. Dirk Voorhoof, Ghent University, Belgium, Copenhagen University, Denmark and Legal Human Academy In: Inter-American and European Human Rights Journal, 2010 (in press);

[36] FREEDOM OF EXPRESSION UNDER THE EUROPEAN HUMAN RIGHTS SYSTEM FROM SUNDAY TIMES (N° 1) V. U.K. (1979) TO HACHETTE FILIPACCHI ASSOCIÉS ("ICI PARIS") V. FRANCE (2009) Prof. Dirk Voorhoof, Ghent University, Belgium, Copenhagen University, Denmark and Legal Human Academy In: Inter-American and European Human Rights Journal, 2010 (in press);

[37] FREEDOM OF EXPRESSION UNDER THE EUROPEAN HUMAN RIGHTS SYSTEM FROM SUNDAY TIMES (N° 1) V. U.K. (1979) TO HACHETTE FILIPACCHI ASSOCIÉS ("ICI PARIS") V. FRANCE (2009) Prof. Dirk Voorhoof, Ghent University, Belgium, Copenhagen University, Denmark and Legal Human Academy In: Inter-American and European Human Rights Journal, 2010 (in press);

[38] See ECtHR (Judgment) 17 December 2004, Case No. 49017/99, Pedersen and Baadsgaard v. Denmark and ECtHR (Judgment) 20 April 2006, Case No. 47579/99, Raichinov v. Bulgaria. For a solid introduction, see E. Dommering, "Article 10 of the Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR): Freedom of Expression", in O. Castendyk,

Personal data, as a matter of public interest, has already been treated by such cases as the case Hachette Filipacchi Associés ("Ici Paris") v. France[39]. In a summary by D.Vorhoof[40] the case facts are such: the Court was called upon to settle a conflict of fundamental rights between the right of privacy, including the right of one's reputation and image (Article 8 of the Convention) and a publishing company's right to freedom of expression, following the publication of an article in the magazine "Ici Paris" about the French (ex-) rock star Johnny Hallyday. The article had focused on the financial difficulties and the extravagant tastes of Mr. Hallyday. The French courts considered the article, which was also illustrated with some photographs, as breaching the right to respect the private life of Mr. Hallyday and disrespecting the right of his image. The publishing company was ordered by the Court of Appeal to pay EUR 20,000 in damages to Mr. Hallyday, together with costs and expenses. Referring to several characteristics of the article, its content and its context, the European Court came to the conclusion that the limits attached to the exercise of journalistic freedom in a democratic society had not been overstepped by the article in "Ici Paris," although the Court recognized that the article did not contribute to any debate of public interest for society. The European Court was of the opinion that the French courts, although having a broader margin of appreciation under these conditions, in their assessment of the publishing company's liability had not struck a fair balance between the conflicting interests at stake. The Court concluded that there had been a violation of Article 10 of the Convention.

In its conclusions,[41] the European Court made clear that in a democratic society, in addition to the press, Nongovernmental organizations (NGOs), campaign groups or organizations, with a message outside the mainstream must be able to carry on their activities effectively and be able to rely on a high level of freedom of expression, as there is "a strong public interest in enabling such groups

---

E. Dommering and A. Scheuer (eds.), European Media Law (Austin, Welters Kluwer 2008) p. 35-80 and E. Barendt, Freedom of Speech (Oxford,
Oxford University Press 2005).

[39] ECtHR (Judgment) 23 July 2009, Case No. 12268/03, Hachette Filipacchi Associés ("Ici Paris") v. France.

[40] http://www-ircm.u-strasbg.fr/seminaire_oct2008/docs/Summariesrecentcases.Voorhoof.pdf

[41] FREEDOM OF EXPRESSION UNDER THE EUROPEAN HUMAN RIGHTS SYSTEM FROM SUNDAY TIMES (N° 1) V. U.K. (1979) TO HACHETTE FILIPACCHI ASSOCIÉS ("ICI PARIS") V. FRANCE (2009) Prof. Dirk Voorhoof, Ghent University, Belgium, Copenhagen University, Denmark and Legal Human Academy In: Inter-American and European Human Rights Journal, 2010 (in press);

and individuals outside the mainstream to contribute to the public debate by disseminating information and ideas on matters of general public interest..."[42]

In a democratic society, public authorities are to be subjected to permanent scrutiny by citizens, and anyone has to have the right to draw the public's attention to situations that they consider unlawful.[43]

Particular attention is paid to the public interest involved in the disclosure of information, contributing to debate on matters of public interest: "In a democratic system the acts or omissions of government must be subject to the close scrutiny not only of the legislative and judicial authorities but also of the media and public opinion. The interest which the public may have in particular information can sometimes be so strong as to override even a legally imposed duty of confidence."[44]

In such circumstances a journalist, a civil servant, an activist, or a staff member of an NGO should not be prosecuted or sanctioned because of breach of confidentiality or the use of illegally obtained documents.[45]

"The Court has accepted that the interest in protecting the publication of information originating from a source which obtained and retransmitted the information unlawfully may in certain circumstances outweigh those of an individual or an entity, private or public, in maintaining the confidentiality of the information. A newspaper that has published illegally gathered emails between two public figures, directly related to a public discussion on a matter of serious public

---

[42] ECtHR (Judgment) 23 September 1998, Case No. 24838/94, Steel and Others v. UK. See also ECtHR (Judgment) 25 August 1998, Case No. 25181/94, Hertel v. Switzerland; ECtHR (Judgment) 28 June 2001, Case No. 24699/94, VGT Verein gegen Tierfabriken v. Switzerland; ECtHR (Judgment) 4 October 2007, Case No. 32772/02, VGT Verein gegen Tierfabriken (n° 2) v. Switzerland; ECtHR (Judgment) 27 May 2004, Case No. 57829/00, Vides Aizsardzības Klubs v. Latvia and ECtHR (Judgment) 7 November 2006, Case No. 12697/03, Mamère v. France. See also ECtHR (Judgment) 29 October 1992, Case No. 14234/88; 14235/88,
Open Door and Dublin Well Women v. Ireland; ECtHR (Judgment) 25 November 1999, Case No. 25594/94, Hashman and Harrup v. UK; ECtHR (Judgment) 20 September 2007, Case No. 57103/00, Çetin and akar v. Turkey and ECtHR (Judgment) 3 February 2009, Case No. 31276/05, Women on Waves v. Portugal.

[43] ECtHR (Judgment) 27 May 2004, Case No. 57829/00, Vides Aizsardzības Klubs v. Latvia.

[44] ECtHR, Grand Chamber (Judgment) 12 February 2008, Case No. 14277/04, Guja v. Moldova.

[45] ECtHR (Judgment) 21 January 1999, Case No. 29183/95, Fressoz and Roire v. France; ECtHR, Dammann v. Switzerland, 25 April 2006; ECtHR (Judgment) 7 June 2007, Case No. 1914/02, Dupuis and Others v. France; ECtHR (Judgment) 26 July 2007, Case No. 64209/01, Peev v. Bulgaria and ECtHR, Grand Chamber (Judgment) 12 February 2008, Case No. 14277/04, Guja v. Moldova. See also ECtHR (Judgment) 19 December 2006, Case No. 62202/00, Radio Twist v. Slovakia.

concern, can be shielded by Article 10 of the Convention against claims based on the right of privacy as protected under Article 8 of the Convention".[46]

As shown by case law,[47] especially in cases where information is published on alleged corruption, fraud or illegal activities in which politicians, civil servants or public institutions are involved, journalists, publishers, media and NGOs can count on the highest standards of protection of freedom of expression. The Court has emphasized that "in a democratic state governed by the rule of law the use of improper methods by public authority is precisely the kind of issue about which the public has the right to be informed." The Court expressed the opinion that "the press is one of the means by which politicians and public opinion can verify that public money is spent according to the principles of accounting and not used to enrich certain individuals."[48]

Defamation laws and proceedings cannot be justified if their purpose or effect is to prevent legitimate criticism of public officials, or the exposure of official wrongdoing or corruption. A right to sue in defamation for the reputation of officials could easily be abused and might prevent free and open debate on matters of public interest or scrutiny of the spending of public money.[49]

As concluded by E. Werkers and P. Valcke in the European Journal of Consumers Law[50], the facts in the case of *Frassoz and Roire v. France*[51] were quite similar to the Goodwin case. Both the journalist and director of the weekly newspaper *'Le Canard enchaine'* had been sued for the publication of an article which was based upon confidential tax files of Peugeot's chairman. The fact that the journalists had received and handled stolen photocopies, obtained through a breach of professional confidence by an unidentified tax official sufficed for the French courts to sentence them to fines and the payment of damages. The E.C.H.R. consented with the journalists that the debate the article had stirred went beyond the Peugeot chairman as

[46] ECtHR (Decision), 16 June 2009, Case No. 38079/06, Jonina Benediktsdóttir v. Iceland. See also ECtHR (Judgment) 21 January 1999, Case No. 29183/95, Fressoz and Roire v. France and ECtHR (Judgment) 19 December 2006, Case No. 62202/00, Radio Twist v. Slovakia.

[47] FREEDOM OF EXPRESSION UNDER THE EUROPEAN HUMAN RIGHTS SYSTEM FROM SUNDAY TIMES (N° 1) V. U.K. (1979) TO HACHETTE FILIPACCHI ASSOCIÉS ("ICI PARIS") V. FRANCE (2009) Prof. Dirk Voorhoof, Ghent University, Belgium, Copenhagen University, Denmark and Legal Human Academy In: Inter-American and European Human Rights Journal, 2010 (in press);

[48] ECtHR (Judgment) 14 November 2008, Case No. 9605/03, Krone Verlag GmbH & Co (n° 5) v. Austria.

[49] ECtHR (Judgment) 9 June 2009, Case No. 17095/03, Cihan Özturk v. Turkey.

[50] Werkers, E. And Valcke P. (2010), „The journalist's right not to reveal his information sources: continuing battle or truce established?" European Journal of Consumers Law (EJCL) (in press)

[51] E.C.H.R. Fressoz and Roire v. France, 21 January 1999, www.echr.coe.int § 50.

an individual and concerned the management of the company he ran, a topic of public interest. The Court did not accept the objective to protect the fiscal confidentiality to be an overriding requirement, especially since the information was already publicly accessible, and thus, not strictly confidential. The conviction could not be justified and violated Article 10 of the Convention, namely the right of journalists to divulge information on issues of general interest provided they act in good faith and on an accurate factual basis and provide reliable and precise information in accordance with the ethics of journalism. The publication of the tax assessment was deemed to be relevant to the subject matter and to the credibility of the information supplied.[52]

Previously it has been shown,[53] that the Court looks at a set of aspects of a case before deciding whether or not an interference with the right to freedom of expression of the applicant(s) is necessary in a democratic society. This "contextualization" of its law-finding implies that the Court focuses on the case in its different aspects," in the light of the case as a whole." To this end, the Court will take into account who is invoking the right to freedom of expression, what was published, broadcasted or imparted, who was eventually criticized or insulted, how the opinions or statements were formulated or what medium was used, to whom the message was directed or who could receive the information, when something was published, broadcasted or imparted, where and under which circumstances something was made public, with what intention information was made public or allegations or opinions were formulated, and what the possible effect or impact of the message was. The Court finally will also take into account the character of the interference or the severity or proportionality of the sanctions, before finally deciding whether or not an interference with the right to freedom of expression amounted to a violation of Article 10 of the Convention.

When analyzing the concrete case of Ilmars Poikans and the state action taken against him to establish his activities classified as criminal, it is necessary to take into account the case law and the judicature in European Court of Human Rights and the

[52] Werkers, E. And Valcke P. (2010), „The journalist's right not to reveal his information sources: continuing battle or truce established?" European Journal of Consumers Law (EJCL) (in press)
[53] FREEDOM OF EXPRESSION UNDER THE EUROPEAN HUMAN RIGHTS SYSTEM FROM SUNDAY TIMES (N° 1) V. U.K. (1979) TO HACHETTE FILIPACCHI ASSOCIÉS ("ICI PARIS") V. FRANCE (2009) Prof. Dirk Voorhoof, Ghent University, Belgium, Copenhagen University, Denmark and Legal Human Academy In: Inter-American and European Human Rights Journal, 2010 (in press);

precedent of establishing whether the concrete interference was necessary in a democratic society.

In analyzing the judgment of December 19, 2006, Radio Twist v. Slovakia, (leaked recordings of telephone conversation with a politician, news programme on radio, privacy, apology) [54] the Strasbourg Court considered the conviction of a radio station as a violation of the freedom of expression guaranteed by Article 10 of the Convention. The applicant, Radio Twist is a radio broadcasting company that was convicted for broadcasting in a news programme the recording of a telephone conversation between the State Secretary at the Ministry of Justice and the Deputy Prime Minister. The recording was accompanied by a commentary, clarifying that the recorded dialogue related to a politically influenced power struggle in June 1996 between two groups which had an interest in the privatization of a major national insurance provider. Mr. D., the Secretary at the Ministry of Justice subsequently filed a civil action against Radio Twist for protection of his personal integrity. He argued that Radio Twist had broadcast the telephone conversation despite the fact that it had been obtained in an illegal manner. Radio Twist was ordered by the Slovakian courts to offer Mr. D. a written apology and to broadcast that apology within 15 days. The broadcasting company was also ordered to pay compensation for damage of a non-pecuniary nature, as the Slovakian courts considered the dignity and reputation of Mr. D. as a public official tarnished. The broadcasting of the illegally tapped conversation was considered as especially unjustified and an interference in the personal rights of Mr. D., as the protection of privacy also extends to telephone conversations of public officials. The Strasbourg Court however disagrees with these findings by the Slovakian Courts. Referring to the general principles that the ECtHR has developed in its case law regarding freedom of expression in political matters, the essential function of the press in a democratic society, and regarding the limits of acceptable criticism of politicians, the Court emphasizes that the context and content of the recorded conversation was clearly political and that the recording and commentary contained no aspects of any private-life dimension of the politicians concerned. Furthermore the Court refered to the fact that the news reporting by Radio Twist did not contain untrue or distorted information and that the reputation of Mr. D. was not

[54] http://www-ircm.u-strasbg.fr/seminaire_oct2008/docs/Summariesrecentcases.Voorhoof.pdf

tarnished by the impugned broadcast, as he was shortly later elected as a judge of the Constitutional Court.

The Court pointed out that Radio Twist was sanctioned mainly for the mere fact of having broadcast information which someone else had obtained illegally and had forwarded to the radio station. The Court was however, not convinced that the mere fact that the recording had been obtained by a third person contrary to the law could deprive the broadcasting company of its Article 10 rights guaranteed by the which Convention. The Court also noted that at no stage was it alleged that the broadcasting company or its employees or agents were in any way liable for the recording or that its journalists transgressed the criminal law when obtaining or broadcasting the material. The Court observes that there is no indication that the journalists of Radio Twist acted in bad faith or that they pursued any objective other than reporting on matters which they felt obliged to make available to the public. For these reasons the Court came to the conclusion that by broadcasting the telephone conversation in question, Radio Twist did not interfere with the reputation and rights of Mr. D. in a manner that could justify the sanction imposed on it. Hence, the interference with its rights to impart information did not correspond to a pressing social need. The interference being not necessary in a democratic society amounted to a violation of Article 10 of the Convention.[55]

The case of Sdruženi Jihočeské Matky v. Czech Republic[56] on July 10, 2006 dealt with access to public documents, principle, restrictions, and inadmissible information. The ECtHR at several occasions has recognized "the right of the public to be properly informed" and "the right to receive information", but until recently the Court was very reluctant to derive from Article 10 of the European Convention on Human Rights a right to have access to public or administrative documents.

In the cases of Leander v. Sweden (1987), Gaskin v. United Kingdom (1989) and Sîrbu v. Moldova (2004)) the Strasbourg Court has indeed recognized "that the public has a right to receive information as a corollary of the specific function of journalists, which is to impart information and ideas on matters of public interest". The Court however was of the opinion that the freedom to receive information

---

[55] ECtHR (Fourth Section), Radio Twist S.A. v. Slovakia, Application no. 62202/00 of 19 December 2006

[56] http://www-ircm.u-strasbg.fr/seminaire_oct2008/docs/Summariesrecentcases.Voorhoof.pdf

basically prohibits a government from restricting a person from receiving information that others wish or may be willing to impart to him. It was decided in these cases that the freedom to receive information as guaranteed by Article 10 could not be construed as imposing on a State positive obligations to disseminate information or to disclose information to the public. In its decision on the admissibility the ECtHR for the first time applied Article 10 of the Convention in a case where a request of access to administrative documents was refused by the authorities. The case concerns a refusal to give an ecologist NGO access to documents and plans regarding a nuclear power station in Temelin, Czech Republic. Although the Court was of the opinion that there has not been a breach of Article 10, it explicitly recognized that the refusal by the Czech authorities is to be considered as an interference with the right to receive information as it is guaranteed by Article 10 of the Convention. Hence, the refusal must meet the conditions set forth in Article 10 § 2.

In the case of Sdruženi Jihočeské Matky v. Czech Republic the Court refers to its traditional case law, emphasizing the freedom to receive information. The Court is also of the opinion that it is difficult to derive from Article 10 a general right to have access to administrative documents. The Court however recognizes that the refusal to give access to administrative documents, in case relating to a nuclear power station, is to be considered as interference in the applicant's right to receive information. Because the Czech authorities had motivated in a pertinent and sufficient way the refusal to give access to the requested documents, the Court was of the opinion that in this case there has been no breach of Article 10 § 2 of the Convention. The refusal was justified for the protection of the rights of others (industrial secrets), in the interest of national security (risk of terrorist attacks) and for the protection of health. The Court also emphasized that the request to have access to essentially technical information about the nuclear power station did not reflect a matter of public interest. For these reasons, it was obvious that there hadn't been an infringement of Article 10 of the Convention and hence the Court declared the application inadmissible. The decision of 10 July 2006 in the case of Sdruženi Jihočeské Matky is important however as it contains an explicit and undeniable recognition of the application of Article 10 in cases of a refusal of a request to have access to public or administrative documents. The right of access to administrative documents is not an absolute one and can indeed be restricted under the conditions of Article 10 § 2, which implies that such a refusal must be prescribed by law, have a legitimate aim and must be necessary

in a democratic society. The decision of the Court of 10 July 2006 gives additional support and opens new perspectives for citizens, journalists and NGO's for having access to administrative documents in matters of public interest.[57]

In the case of White v. Sweden, 19 September 2006 (presumption of innocence, right of privacy, public interest) as described[58] in 1996, the two main evening newspapers in Sweden, Expressen and Aftonbladet, published a series of articles in which various criminal offences were ascribed to Anthony White, a British citizen residing in Mozambique. The articles also included an assertion that he had murdered Olof Palme, the Swedish Prime Minister, in 1986. Mr. White was a well-known figure whose alleged illegal activities had already been the focus of media attention. The newspapers also reported statements of individuals who rejected the allegations made against Mr. White. In interview published in Expressen, Mr. White denied any involvement in the alleged offences. Mr. White brought a private prosecution against the editors of the newspapers for defamation under the Freedom of Press Act and the Swedish Criminal Code. The District Court of Stockholm acquitted the editors and found that it was justifiable to publish the statements and pictures, given that there was considerable public interest in the allegations. It further considered that the newspapers had a reasonable basis for the assertions and that they had performed the checks that were called for in the given circumstances, taking into regard the constraints of a fast news service. The Court of Appeal upheld the District Court's decision.

Mr. White complained before the ECtHR in Strasbourg that the Swedish courts had failed to provide due protection for his name and reputation. He relied on Article 8 (right to respect for private and family life). The European Court found that a fair balance has to be struck between the competing interests, freedom of expression (Article 10) and the right to respect for privacy (Article 8), also taking into account that under Article 6 § 2 of the Convention individuals have a right to be presumed innocent of any criminal offence until proven guilty in accordance to the law. The Court first noted that as such the information published in both newspapers constituted defamation to the applicant. The statements clearly tarnished his

---

[57] Decision by the ECtHR (Fifth Section), Sdruženi Jihočeské Matky v. Czech Republic, Application no. 19101/03 of 10 July 2006

[57] http://www-ircm.u-strasbg.fr/seminaire_oct2008/docs/Summariesrecentcases.Voorhoof.pdf

reputation and disregarded his right to be presumed innocent until proven guilty as it appeared that Mr. White had not been convicted of any of the offences ascribed to him.

However in the series of articles, the newspapers had endeavored to present an account of the various allegations made which was as balanced as possible and the journalists had acted in good faith. Moreover, the unsolved murder of the former Swedish Prime Minister Olof Palme and the ongoing criminal investigations were matters of serious public interest and concern. The Strasbourg Court considered that the domestic courts made a thorough examination of the case and balanced the opposing interests involved in conformity with Convention standards. The European Court found that the Swedish courts were justified in finding that the public interest in publishing the information in question outweighed Mr White's right to the protection of his reputation. Consequently, there had been no failure on the part of the Swedish State to afford adequate protection of the applicant's rights. For these reasons, the Court considered that there had been no violation of Article 8.[59]

As it was established[60] in the case of Dupuis and others v. France (confidential information, breach of confidentiality, reporting on judicial investigation, media coverage) in a judgment of 7 June 2007 the Court unanimously was of the opinion that the French authorities have violated the freedom of expression of two journalists and a publisher (Fayard). Both journalists were convicted of using confidential information published in their book "The Ears of the President" (Les Oreilles du President). The book focused on the "Elysée eavesdropping operations", an illegal system of telephone tapping and record-keeping, orchestrated by the highest office of the French State and directed against numerous figures from civil society, including journalists and lawyers. The French Courts found the two journalists, Dupuis and Pontaut, guilty of the offence of using information obtained trough a breach of the confidentiality of the investigation or of the professional confidentiality. It was also argued that the publication could be detriment for the presumption of innocence of Mr. G.M., the deputy director of President Mitterrand's private office at the material time, who was placed under formal investigation for breach of privacy under suspicion of being the responsible person for the illegal telephone tapping.

---

[59] ECtHR (Second Section), White v. Sweden, Application no. 42435/02 of 19 September 2006

[60] http://www-ircm.u-strasbg.fr/seminaire_oct2008/docs/Summariesrecentcases.Voorhoof.pdf

The European Court observed that the subject of the book concerned a debate of considerable public interest, an affair of state, which was of interest to public opinion. The Court also referred to the status of Mr. G.M. as a public person, clearly involved in political life at the highest level of the executive while the public had a legitimate interest to be informed about the trial, and in particular, about the facts dealt with or revealed in the book. The Court found it legitimate that special protection should be granted to the confidentiality of the judicial investigation, in view of the stakes of criminal proceedings, both for the administration of justice and for the right of persons under investigation to be presumed innocent. However, at the time when the book was published, the case had already undergone wide media coverage and it was already well known that Mr. G.M. had been placed under investigation in this case. Hence, the protection of the information on account of its confidentiality did not constitute an overriding requirement.

The Court also questioned whether there was still an interest in keeping information confidential when it had already been at least partly made public and was likely to be widely known, having regard to the media coverage of the case. The Court further considered that it is necessary to take the greatest care in assessing the need to punish journalists for using information obtained through a breach of the confidentiality of an investigation or of professional confidentiality when those journalists are contributing to a public debate of such importance, thereby playing their role as "watchdogs" of democracy. According to the Court, the journalists had acted in accordance with the standards governing their profession as journalists: the impugned publication was relevant not only to the subject matter but also to the credibility of the information supplied.

Lastly, the Court underlined that the interference with freedom of expression might have a chilling effect on the exercise of that freedom – an effect that the relatively moderate nature of the fine, as in the present case, would not suffice to negate. As the conviction of the two journalists had constituted a disproportionate interference with their right to freedom of expression it was therefore not necessary in a democratic society. Accordingly, the Court found that there has been a violation of Article 10 of the Convention. [61]

[61] ECtHR (Third Section), case of Dupuis and others v. France, Application no. 1914/02 of 7 June 2007

In the case of Guja v. Moldova[62], February 12, 2008 the protection of whistle blower, matter of public interest, conditions for protecting whistle blowing under Art. 10 Convention and so forth were analyzed. The ECtHR delivered a judgment on this very particular and interesting case, concerning the position of a "whistle-blower" who leaked two letters to the press and was subsequently dismissed. The Court held that the divulgence of the internal documents to the press was in this case protected by Article 10 of the Convention guaranteeing the right to freedom of expression, including the right to receive and impart information and ideas. The applicant, Mr. Guja, was Head of the Press Department of the Moldovan Prosecutor General's Office, before he was dismissed, on the grounds that he had handed over two secret letters to a newspaper and that, before doing so, he had failed to consult the heads of other departments of the Prosecutor General's Office, a behavior which constituted a breach of the press department's internal regulations. Guja was of the opinion that the letters were not confidential and that, as they revealed that the Deputy Speaker of Parliament, Vadim MiSin, who had exercised undue pressure on the Public Prosecutor's Office, he had acted in line with the President's anti-corruption drive and with the intention of creating a positive image of the Office. Guja brought a civil action against the Prosecutor General's Office seeking reinstatement, but his request failed. Relying on Article 10 of the Convention, he complained to the Strasbourg Court about his dismissal.

The European Court held that, given the particular circumstances of the case, external reporting, even to a newspaper, could be justified, as the case concerned the pressure by a high-ranking politician on pending criminal cases. At the same time, the Public Prosecutor had given the impression that he had succumbed to political pressure. The Court also referred to the reports of international non-governmental organizations (the International Commission of Jurists, Freedom House, and the Open Justice Initiative), which had expressed concern about the breakdown of the separation of powers and the lack of judicial independence in Moldova. Court was of the opinion that there is no doubt that these are very important matters in a democratic society, about which the public has a legitimate interest in being informed and which fall within the scope of political debate.

[62] http://www-ircm.u-strasbg.fr/seminaire_oct2008/docs/Summariesrecentcases.Voorhoof.pdf

The Court considered that the public interest in the provision of information on undue pressure and wrongdoing within the Prosecutor's Office is so important in a democratic society, that it outweighs the interest in maintaining public confidence in the Prosecutor General's Office. Open discussion of topics of public concern is essential to democracy and it is of great importance if members of the public are discouraged from voicing their opinions on such matters. The Court, being of the opinion that Guja had acted in good faith, finally noted that it was the heaviest sanction possible (dismissal) that had been imposed on the applicant. The sanction not only had negative repercussions on the applicant's career, but could also have a serious chilling effect on other employees from the Prosecutor's Office and discourage them from reporting any misconduct. Moreover, in view of the media coverage of the applicant's case, the sanction could also have a chilling effect on other civil servants and employees. Being mindful of the importance of the right to freedom of expression on matters of general interest, of the right of civil servants and other employees to report illegal conduct and wrongdoing at their place of work, the duties and responsibilities of employees towards their employers and the right of employers to manage their staff, and having weighed up the other different interests involved in the applicant's case, the Court came to the conclusion that the interference with the applicant's right to freedom of expression, in particular his right to impart information, was not "necessary in a democratic society". Accordingly, there had been a violation of Article 10 of the Convention.[63]

8. Conclusions

1. In the decision of July 21, 2011 the State Police Central Criminal Police Department Economic Section investigator Jelena Fedeneva declared Ilmars Poikāns a suspect in criminal activity, in accordance with Criminal Law Section 241, Paragraph 3.

The process of changing the Uniform Resource Locator (URL), in the concrete case of the website, by simply altering a number in the web address, then requesting the document from the web server with this new URL, and then downloading of the documents from the web-server, can not be classified as

[63] ECtHR (Grand Chamber), Guja v. Moldova, Application no. 14277/04 of 12 February 2008

arbitrary (without the relevant permission or utilizing the rights granted to another person) access of an automated data processing system by breaching data processing protective systems.

In addition, in order to prosecute I.Poikans for criminal liability on the basis of Criminal Law Section 241, Paragraph 3, the actions of I.Poikans would have to fully comply with those set forth as punishable by the Section and would have had to cause substantial harm. None of the actions committed by Ilmars Poikans have resulted in substantial harm in line with the understanding put forward by „The Criminal Law Implementation and Realization Order" Section 23, Paragraph 1, which states that one is criminally liable for the offence committed in accordance with the Criminal Law, if as a result of the offence committed not only there substantial material loss but also other interests or rights protected by the law are also threatened or such threat is substantial. As Paragraph 2 specifies, substantial material loss is defined as material loss which at the time of the incident is more than five time the minimal monthly wage of the Republic of Latvia (in this case 900.00 LVL or 1280.00 EUR).

Therefore, Ilmars Poikans can not be considered as criminally liable in accordance with the Criminal Law Section 241 Paragraph 3, as I.Poikans actions do not correspond with the norms set forth by the law and there has been no material hard caused.

2. In the decision of July 21, 2011, the State Police Central Criminal Police Department Economic Sector investigator Jelena Fedeneva, declared Ilmars Poikans a suspect in criminal activity, in accordance with Criminal Law Section 145 Paragraph 1.

The activities of Ilmars Poikans, when understood in line with freedom of expression rights in the name of the public interests, can not be acknowledged as illegal activities involving personal data of a natural person.

Moreover, none of the activities have caused any harm that would have resulted is substantial material loss, or threatened other interests or rights protected by law nor has such threat been substantial. There has been no substantial material loss caused that at the time of the incident is more than five time the minimal monthly wage of the Republic of Latvia (in this case 900.00

LVL or 1280.00 EUR) as stipulated by „The Criminal Law Implementation and Order" Section 23.

As it is stated by Latvian Personal Data Protection Law, Section 3, Paragraph 3, the Law shall not apply to the information systems made by natural persons in which personal data are processed for personal or household and family purposes and in which the personal data collected are not disclosed to other persons. The published lists of the employees and salaries can not be acknowledged as publishing personal data, as this did not identify concrete person to whom the published data relates to.

The list published by Ilmars Poikans identifying the names and salaries of concrete persons was done under the protection afforded by the Law on Prevention of Conflict of Interest in Activities of Public Officials in Latvia. The published data was already publically available and accessible to anyone interested in accordance with the legislation of Latvia.

3. In the decision of July 21, 2011, the State Police Central Criminal Police Department Economic Sector investigator Jeļena Fedeņeva, declared Ilmars Poikāns a suspect in criminal activity, in accordance with Criminal Law Section 200, Paragraph 2.

In analyzing the activities of Ilmars Poikans, in accordance with the materials of the case, it can be concluded that none of the activities of I.Poikans could be referred to as the unauthorized acquisition of economic, scientific technical, or other information in which there are commercial secrets, for use or disclosure by himself or herself or another person, or commit unauthorized disclosure of such information to another person for the same purpose, as well as to commit unauthorized disclosure of inside information of the financial instrument market.

In the concrete case, the information obtained by I.Poikans can not be classified as commercial secrets, the acquisition of which was for self use or for use by other persons. In addition, of the acquired information only limited excerpts were published – specifically the amount of salary paid. In turn, the acquired information was kept in a hard disk, which was in constant possession of I.Poikans, and this information was in reality only stored not used.

In publishing the salaries of State and regional authority employees, Ilmars Poikans urged the public to analyze the data supplied by him and to determine from it if the reforms they had been subjected to were fair. In presenting the information in a way that the public could understand it, I.Poikans was acting in public interest. The public has a right to know where their tax payer money is being spent. The interference from the governing authorities was against his right to impart the information and was not "necessary in a democratic society". Moreover, such action from the Latvian authorities violated Ilmars Poikans rights to freedom of expression.

Authors Concluding Remarks

The author, as a sworn attorney and information communication technology and media law expert, considers it imperative to define and implement a clear and unmistakable legal framework. Criminally liable offenders have to be held accountable to the full extent of the law, however, the punishable actions have to correspond to the legal norms set forth and take legal precedent into account, and the concrete offence committed has to be either an action restricted or forbidden by the law.

Taking into account the circumstances of the case analyzed, the author concludes that Ilmars Poikans actions do not correspond to the offences

envisioned as criminally liable under the Criminal Law Section 145, Paragraph 1; Section 200, Paragraph 2; or Section 241, Paragraph 3. Because of I.Poikans actions there has been no substantial harm caused either to the system, form which the information was acquired, nor to the persons whose information was acquired.

Considering the case material, and the fact that the goal of I.Poikans was to inform the society at large of the way in which the State was going about fulfilling its promises in regard to tax payer money, if in this criminal process Ilmars Poikans was to be held criminally liable in accordance with the Criminal Law Section 145, Paragraph 2 and/or Section 200, Paragraph 2 and/or Section 241, Paragraph 3, it is the opinion of the author that the activities of I.Poikans would be restricted through illegitimate methods. The penalty would only serve as precedent to preclude similar cases in the future. Given that in this case, the State also should be held partially responsible for the actions preformed by I.Poikans with the goal of informing society, such methods of restriction or punishment would be judged as illegitimate by the firmly established European court precedent.

9. Bibliography

1. The Criminal Law, from 17.06.1998.;
2. Personal Data Protection Law, from 23.03.2000.;
3. 15.10.1998. likums "Par Krimināllikuma spēkā stāšanās laiku un kārtību" ("LV", 331/332 (1392/1393), 04.11.1998.; Ziņotājs, 23, 03.12.1998.);
4. Law on Prevention of Conflict of Interest in Activities of Public Officials in Latvia, from 25.04.2002;
5. „Krimināllikuma zinātniski praktiskais komentārs 3" Sevišķā daļa, Zinātniskais redaktors Dr.Habil. Jur. Prof. U.Krastiņš, Firma „AFS", Rīga, 2007;
6. FREEDOM OF EXPRESSION UNDER THE EUROPEAN HUMAN RIGHTS SYSTEM FROM SUNDAY TIMES (N° 1) V. U.K. (1979) TO HACHETTE FILIPACCHI ASSOCIÉS ("ICI PARIS") V. FRANCE (2009) Prof. Dirk Voorhoof, Ghent University, Belgium, Copenhagen University,

Denmark and Legal Human Academy In: Inter-American and European Human Rights Journal, 2010 (in press);

7. Werkers, E. And Valcke P. (2010), „The journalist's right not to reveal his information sources: continuing battle or truce established?" European Journal of Consumers Law (EJCL) (in press);
8. ECtHR (Judgment) 17 December 2004, Case No. 49017/99, Pedersen and Baadsgaard v. Denmark and ECtHR (Judgment) 20 April 2006, Case No. 47579/99, Raichinov v. Bulgaria. For a solid introduction, see E. Dommering, "Article 10 of the Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR): Freedom of Expression", in O. Castendyk, E. Dommering and A. Scheuer (eds.), European Media Law (Austin, Welters Kluwer 2008) p. 35-80 and E. Barendt, Freedom of Speech (Oxford, Oxford University Press 2005).
9. ECtHR (Judgment) 23 July 2009, Case No. 12268/03, Hachette Filipacchi Associés ("Ici Paris") v. France;
10. ECtHR (Judgment) 23 September 1998, Case No. 24838/94, Steel and Others v. UK. See also ECtHR (Judgment) 25 August 1998, Case No. 25181/94, Hertel v. Switzerland; ECtHR (Judgment) 28 June 2001, Case No. 24699/94, VGT Verein gegen Tierfabriken v. Switzerland; ECtHR (Judgment) 4 October 2007, Case No. 32772/02, VGT Verein gegen Tierfabriken (n° 2) v. Switzerland; ECtHR (Judgment) 27 May 2004, Case No. 57829/00, Vides Aizsardzības Klubs v. Latvia and ECtHR (Judgment) 7 November 2006, Case No. 12697/03, Mamère v. France. See also ECtHR (Judgment) 29 October 1992, Case No. 14234/88; 14235/88, Open Door and Dublin Well Women v. Ireland; ECtHR (Judgment) 25 November 1999, Case No. 25594/94, Hashman and Harrup v. UK; ECtHR (Judgment) 20 September 2007, Case No. 57103/00, Çetin and akar v. Turkey and ECtHR (Judgment) 3 February 2009, Case No. 31276/05, Women on Waves v. Portugal;
11. ECtHR (Judgment) 27 May 2004, Case No. 57829/00, Vides Aizsardzības Klubs v. Latvia;
12. ECtHR (Judgment) 17 February 2004, Case No. 44158/98, Gorzelik v. Poland;
13. ECtHR, Grand Chamber (Judgment) 12 February 2008, Case No. 14277/04, Guja v. Moldova;
14. ECtHR (Judgment) 21 January 1999, Case No. 29183/95, Fressoz and Roire v. France; ECtHR, Dammann v. Switzerland, 25 April 2006; ECtHR (Judgment) 7 June 2007, Case No. 1914/02, Dupuis and Others v. France; ECtHR (Judgment) 26 July 2007, Case No. 64209/01, Peev v. Bulgaria and ECtHR, Grand Chamber (Judgment) 12 February 2008, Case No. 14277/04, Guja v. Moldova. See also ECtHR (Judgment) 19 December 2006, Case No. 62202/00, Radio Twist v. Slovakia;
15. ECtHR (Decision), 16 June 2009, Case No. 38079/06, Jonina Benediktsdóttir v. Iceland. See also ECtHR (Judgment) 21 January 1999, Case No. 29183/95, Fressoz and Roire v. France and ECtHR (Judgment) 19 December 2006, Case No. 62202/00, Radio Twist v. Slovakia;
16. ECtHR (Judgment) 14 November 2008, Case No. 9605/03, Krone Verlag GmbH & Co (n° 5) v. Austria;
17. ECtHR (Judgment) 9 June 2009, Case No. 17095/03, Cihan Özturk v. Turkey;
18. E.C.H.R. Fressoz and Roire v. France, 21 January 1999, www.echr.coe.int § 50;

19. ECtHR (Fourth Section), Radio Twist S.A. v. Slovakia, Application no. 62202/00 of 19 December 2006;
20. Decision by the ECtHR (Fifth Section), Sdruženi Jihočeské Matky v. Czech Republic, Application no. 19101/03 of 10 July 2006;
21. ECtHR (Second Section), White v. Sweden, Application no. 42435/02 of 19 September 2006;
22. ECtHR (Third Section), case of Dupuis and others v. France, Application no. 1914/02 of 7 June 2007;
23. ECtHR (Grand Chamber), Guja v. Moldova, Application no. 14277/04 of 12 February 2008
24. http://www.nytimes.com/2008/12/15/opinion/15krugman.html;
25. http://freespeechlatvia.blogspot.com/;
26. http://www.movements.org/case-study/entry/a-web-savvy-latvian-uncovers-and-spotlights-public-corruption/;
27. http://www.movements.org/case-study/entry/a-web-savvy-latvian-uncovers-and-spotlights-public-corruption/;
28. http://en.rsf.org/latvia-judicial-authorities-urged-to-end-25-08-2010,38199.html;
29. http://www.tiesibsargs.lv/lat/tiesibsargs/jaunumi/?doc=264;
30. http://www.movements.org/case-study/entry/a-web-savvy-latvian-uncovers-and-spotlights-public-corruption/;
31. http://www.technologyreview.com/wire/24651/page1/;
32. http://en.rsf.org/latvia-judicial-authorities-urged-to-end-25-08-2010,38199.html;
33. http://freespeechlatvia.blogspot.com/2010/05/latvian-tv-investigative-journalists.html;
34. http://en.rsf.org/latvia-judicial-authorities-urged-to-end-25-08-2010,38199.html;
35. http://news.bbc.co.uk/2/hi/technology/8533641.stm;
36. http://latviansonline.com/news/article/7083/;
37. http://www-ircm.u-strasbg.fr/seminaire_oct2008/docs/Summariesrecentcases.Voorhoof.pdf.