Court of Magistrates (Malta)
As A Court of Criminal Judicature

Magistrate Dr. Claire L. Stafrace Zammit B.A. LL.D.

The Police
[Inspector Daniel Zammit]

-vs-

Roswitha Marion Lehner

Case Number: 1317/12

Today, the 24th of September, 2018

The Court,

Having seen that the accused Roswitha Marion Lehner, holder of Identity Card Number 12497A was charged with having, in October 2005 and during the previous months on these Islands, committed several acts by herself at different times, which constitute violations of the same provisions of the law, and were committed in pursuance of the same design, without authorization;

1. Used a computer or any other device or equipment to access any data, software or supporting documentation held in that computer or any other computer, or used, copied or modified any such data, software or supporting documentation;

2. Outputted any data, software or supporting documentation from that computer in which it was held, whether by having it displayed or in any other manner whatsoever;

3. Copied any data, software or supporting documentation to any storage medium or other than that in which it was held or to a different location in the storage medium in which it was held;

4. Prevented or hindered access to any data, software or supporting documentation;

5. Hindered or interrupted the functioning of an information system by inputting computer data, by transmitting damaging, deleting, deteriorating, altering or suppressing such data, or by rendering such data inaccessible;

6. Took possession of or made use of any data, software or supporting documentation;

7. Installed, moved, altered, damaged, deleted, deteriorated, suppressed, destroyed, varied or added to any data, software of supporting documentation or rendered such data inaccessible;

8. Disclosed a password or any other means of access, access code or other access information to any unauthorized person;

9. Used another person's access code, password, user name, electronic mail address or other means of access or identification information in a computer of another person;

10. Disclosed any data, software or supporting documentation that was not required in the course of your duties or by any other law.

Seen that the accused pleaded not guilty to the charges brought against her;

Seen all documentation including all the evidence produced;

Seen statement given voluntarily by the accused dated the twentieth (20th) June of the year two thousand and seven (2007) by the then Inspector Daniel Zammit in the presence of PS 430 Andrew St John but which statement was given without the right of consultation of a lawyer and therefore by virtue of

various European Court judgments and as well as local Constitutional judgments, this court is not taking cognisance of this document;

Seen that these proceedings relate to Article 337C of Chapter 9 of the Laws of Malta thereby referring to computer misuse which was a law introduced in our Criminal Code by Act VII of the year two thousand and ten (2010) and later amended by Act VII of the year two thousand and fifteen (2015);

In these proceedings it is being alleged that the accused accessed illegally to the computer of her husband (by whom she is now separated) and from it she stole certain documents which appertained to him;

In fact in the testimony of her ex husband **Ian Pace** dated the sixteenth (16th) of May of the year two thousand and sixteen (2016), the witness declared that in the year nineteen eighty one (1981) he started working with Compitec Limited as a medical representative of the same company and which provided the same with a computer which was a *Dell Latitude C600* which consisted of a laptop and a docking station. He also declared that he always kept this computer in his matrimonial home since he used to conduct his work mostly from home where he used to live with his wife and son.

He also declared that initially he gave access to the said computer to his wife so that she could use the emails since at the time she didn't have a computer. He also says that shortly he left the matrimonial home in the year two thousand and five (2005) and his computer started crushing. He was living at Holland at the time for a couple of months. He had his computer tested by a local computer technician in Holland whereby he informed him that

something had been done to his computer recently before and that almost all of his files had been copied and removed from his computer. This he said dated approximately September of the year two thousand and five (2005) which was the time when he was sailing on a boat. He says that at the time he left his computer home and it was controlled by a password.

Ian Pace also declared that he kept his password in his head and never gave access to use his computer to anyone. He also says the following:

> *"I asked him how was it possible that most of my files are dated twenty first (21st) September and he said: Does anyone have access to your computer, which I told him with a password no. And he said: Did you know that it's very simple to flip it over, unscrew, take out the hard drive just you got access to all the files, and basically that was how it was done, I didn't know that, a password is just useless. Because all that was done was my files were literally removed from my computer, copied and pasted back, that's why all the files were dated twenty first (21st) September two thousand and five (2005)".*

As a result he concluded that the only person who could have done this job was his wife the accused with the help of a technician Sean Ebejer.

Another witness was heard **Sean Ebejer** who gave his testimony in the sitting dated thirteenth (13th) of February of the year two thousand and seventeen (2017) who is the computer technician whom Ian Pace referred to in his testimony.

Ebejer recounts that way back in the year two thousand and seven (2007) the accused contacted him to access to the computer which he calls as the family computer since he knew both the accused and Ian Pace as being close friends. He says that even though there was a password it wasn't about cracking it but one could only press the *escape* button and access is automatic into *Windows*. He also confirms that the accused had her emails on this computer and what she wanted is to access to her emails and he confirmed this since he was present when she was working on it. He also confirmed that their son Ben also used to work on the same computer and that is why he called it as the family computer.

The Court also heard the oral submissions of both parties which were made in the Maltese language with the consent of the accused;

As was already stated these proceeding refer to the Article relating to Computer Misuse in the Criminal Code namely Art 337C which states that:

> *337C.(1) "A person who without authorisation does any of the following acts shall be guilty of an offence against this article –*
>
> *(a)uses a computer or any other device or equipment to access any data, software or supporting documentation held in that computer or on any other computer, or uses, copies or modifies any such data, software or supporting documentation;*

(b)outputs any data, software or supporting documentation from the computer in which it is held, whether by having it displayed or in any other manner whatsoever;

(c)copies any data, software or supporting documentation to any storage medium other than that in which it is held or to a different location in the storage medium in which it is held;

(d)prevents or hinders access to any data, software or supporting documentation;

(e)hinders or impairs the functioning or operation of a computer system, software or the integrity or reliability of any data;

(ee)hinders or interrupts the functioning of an information system by inputting computer data, by transmitting, damaging, deleting, deteriorating, altering or suppressing such data, or by rendering such data inaccessible;

(f)takes possession of or makes use of any data, software or supporting documentation;

(g)installs, moves, alters, damages, deletes, deteriorates, suppresses, destroys, varies or adds to any data, software or supporting documentation or renders such data inaccessible;

(h)discloses a password or any other means of access, access code or other access information to any unauthorised person;

(i)uses another person's access code, password, user name, electronic mail address or other means of access or identification information in a computer or in any manner infringes any security measure to gain access without authorization to the whole or to any part of an information system;

(j)discloses any data, software or supporting documentation unless this is required in the course of his duties or by any other law;"

This Article of the Criminal Code was based on the Law on Computer Misuse found in UK legislation of 1990 where this law was introduced in the UK to fill in the gaps in the criminal law existing at the time regarding the misuse of computer systems. In fact in the Law Commission's substantive report[1] on computer misuse it was stated that:

"An increasing degree of interest and disquiet has become apparent in recent years in relation to the implications of, and the possible misuse of, the computerization that plays an ever growing role in public, commercial and indeed private life. In this report we are concerned with one aspect of that public concern: the misuse of computers or computer systems by parties other than those entitled to use or control those computers, either by simply seeking access to the computers or amending the information held in them for what

[1] Law Commission, Computer Misuse, Report No 186, Cmnd 819 (Law Commission, 1989).

may be a wide range of ulterior motives. Such conduct can be generically described by the title of this report, 'Computer Misuse'.

In paragraph 2.13 of the same report it was concluded that this law of Computer Misuse was intended to target the so-called "hacking offences" and not the protection of confidential information but rather the integrity of computer systems.

Matthew Richardson in his book titled *Cyber Crime – Law and Practice*[2] lays down which are the elements of this offence in the UK and says:

"The actus reus of the offence under section 1 of the CMA 1990 is substantiated by causing a computer to perform 'any function' in order to secure access to it. In practice, therefore, the actus reus can be substantiated by relatively innocuous acts. . .

Given the common sense meaning of section 1(1) of the CMA 1990 read alongside the interpretative provisions in section 17(2)(c) and (3), a simple act such as opening of a file on a computer can substantiate the offence, even if it is not apparent what (if any) data the file may contain.

The broad scope of the actus reus of the offence under section 1 of the CMA 1990 was illustrated in Ellis v. DPP (No. 1) [2001] EWHC 362 (Admin), in which the appellant appealed by way of case stated three convictions under section 1 for using non-open access

[2] Cyber Crime: Law and Practice – Matthew Richardson; 2014; pg 5

computer facilities at a university. As a graduate of the university, the appellant had been authorized to use only the open access computer facilities at the university (such authorization did not extend to the restricted access facilities). The appellant was able to use the non-open access computers by using terminals which had been logged on to the accounts of bona fide authorized users. He admitted using those computers to browse the internet. Whilst the appellant did not make representations at appeal, it is noted in the judgment that the appellant in his police interview equated such use to picking up and reading someone's discarded newspaper. A skeleton argument submitted by the appellant earlier in the proceedings argued that the browsing did not constitute the 'use' of the computers for the purposes of the CMA 1990 as the appellant had browsed already activated sites, i.e. that he had merely pressed the 'back' button on the internet browser. This argument did not find favour with the Administrative Division and the Appeal was dismissed".

As regards the *mens rea* required for these types of offences, the UK legislation requires the intention by the perpetrator to secure unauthorized access to a computer and cannot be made out of mere recklessness. This act must be made with the specific knowledge that access is unauthorized.

As regards the term "unauthorized", there may be cases where the entire computer system may be unauthorized or where only access to some programs may be authorized and others not. In the illustration by Matthew Richardson quoted earlier in this judgment, reference was made to the case

DPP v. Bignell[3] where two police officers successfully appealed their convictions where they had been originally charged for using the Police National Computer for personal purposes where normally they are only allowed to use for police purposes. The Administrative Division ruled that respondents had had the authority to access the data even though they did not do so for an authorized purpose. In fact the same UK court held the following:

> *"Section 17(5) (a) makes access unlawful provided a person is not entitled to control access set out in section 17(5)(a) and who does not have consent to access of one of the kinds set out in section 17(2)(a) to (d) from any person who is so entitled. If, as the appellant submits, the Commissioner alone has control access, the consent given by him to the respondents to access the computer at the point of entry for any of the kinds set out in section 17(2)(a) to (d), provides them with a defence by virtue of section 17(5)(b) even if the access is for an unlawful purpose. A person does not have control access but who accesses a computer at the point of entry does not commit an offence under section 1 of the Computer Misuse Act if he obtains access of any of the kinds set out in section 17(2)(a) to (d) and he has the consent to do so of a person having control access".*[4]

This judgment is being quoted amply because it has a close resemblance to these proceedings. Here we have a husband and wife using the same computer, even though it is said to be the husband's work computer and the

[3] [1998] 1 Cr App R 1
[4] *DPP v. Bignell* [1998] 1 Cr App R 1, per Astill J 12-13.

husband who has control access gives access to the wife and presumably the son to his computer. It is not clear if at the time when the husband was still in Malta whether the computer was protected by a password and it is not even clear because the parte civile failed to comment about this, whether he expressly prohibited all access to the wife when he was in Holland. His failure to comment about this leads this court to think in the negative so much so that he left his computer in the matrimonial home when he was away.

Another thing is that as the computer technician stated in his testimony, to enter in the *outlook* so that accused could access to her emails needed very little but press the *escape* button thereby no need of cracking passwords or other complicated devices.

As regards the evidence tendered by the prosecution, the only evidence tendered was the testimony of the parte civile Ian Pace and that of Sean Ebejer who is the only independent witness of these proceedings and who testified that accused only used the computer that time to access her emails and this was something that she knew that she could do.

What was outstanding in these proceedings is a complete lack of substantive evidence starting from the testimony of the aggrieved party who was very vague in his version of facts when one time he speaks of the accused allegedly deleting all his files and in another instance he talks about the accused copying the same files. Evidence was not brought for example what type of files were they? If the aggrieved party was acting in *bona fide* and stated that he had retrieved some or all of these files, why didn't he present a

copy of these files or the laptop itself so that it can be examined from a court expert. None of this was done!

Instead all his acts and non facts make this Court to believe that this is a *vendetta* against the wife in order to win something during the separation proceedings. That is why he was forcefully pushing for these proceedings to be ended with as soon as possible.

Furthermore this court cannot assess what type of documents were allegedly manipulated, altered or deleted as he alleges since no evidence was tendered to this effect.

Thereby, having established that the access by the accused was authorized and having this lack of evidence so important for this case to succeed, this Court is not going to deal with the charges one by one since it considers that none of them subsist.

On the above basis considers that none of the charges were proven and that the accused **Roswitha Marion Lehner** cannot be found guilty of them and consequently acquits her from all the charges brought against her.

Dr Claire Stafrace Zammit B.A. LL.D.
Magistrate

Benjamina Mifsud
Deputy Registrar