Tan Chye Guan Charles v Public Prosecutor
[2009] SGHC 128

Case Number : MA 11/2009

Decision Date : 26 May 2009

Tribunal/Court : High Court

Coram : Choo Han Teck J

Counsel Name(s) : Michael Khoo Kah Lip SC and Josephine Low Miew Yin (Michael Khoo & Partners) for the appellant; Gillian Koh-Tan (Attorney-General's Chambers) for the respondent

Parties : Tan Chye Guan Charles — Public Prosecutor

Criminal Procedure and Sentencing – Sentencing – Appeals – Principles governing appellate interference with sentence imposed by trial judge

Criminal Procedure and Sentencing – Sentencing – Computer Misuse Act (Cap 50A, 1998 Rev Ed) – Unauthorised access to computer material – Accused copying file of agency tasked with defence-related matters into thumbdrive – Sentencing considerations applicable

26 May 2009 Judgment reserved.

Choo Han Teck J:

1 The appellant is 37 years old and was the Managing Director of a company called "du Lexbuild International Pte Ltd" ("du Lexbuild"), a defence contractor, that is, a company that was or might be commissioned to produce materials for the Singapore Armed Forces ("SAF"). In early 2007, the Defence Science & Technology Agency ("DSTA") of the Ministry of Defence invited tenders from various contractors, including du Lexbuild, to tender for a contract to build the SAF's Munitions Storage Container System ("MSCS"). Prior to the invitation to tender, the appellant and his colleague met the DSTA project manager in charge of the MSCS. That meeting took place in the lobby of the DSTA office in the Defence Technology Tower Lobby A. The project manager left his laptop computer when he went to answer a telephone call. The appellant took the opportunity and looked at the laptop screen. He recognized a file name displayed on the screen and realized that it might have information useful to him. He inserted his thumb-drive into the laptop and copied the file into the thumb drive by the "drag-and-drop" method. His action was eventually found out and he was charged under s 3(1) of the Computer Misuse Act, Cap 50A (Revised Edition 1998) ("CMA"). He pleaded guilty and was sentenced to three weeks imprisonment and fined $5,000 which was the maximum fine for an offence under s 3(1). Section 3 provides as follows:

> 3-(1) Subject to subsection (2), any person who knowingly causes a computer to perform any function for the purpose of securing access without authority to any program or data held in any computer shall be guilty of an offence and shall be liable on conviction to a fine not exceeding $5,000 or to imprisonment for a term not exceeding 2 years or to both and, in the case of a second or subsequent conviction, to a fine not exceeding $10,000 or to imprisonment for a term not exceeding 3 years or to both.
>
> (2) If any damage is caused as a result of an offence under this section, a person convicted of the offence shall be liable to a fine not exceeding $50,000 or to imprisonment for a term not exceeding 7 years or to both.

(3) For the purposes of this section, it is immaterial that the act in question is not directed at –

(a) any particular program or data;

(b) a program or data of any kind; or

(c) a program or data held in any particular computer.

The appellant appealed against the sentence on the ground that it was manifestly excessive. Mr Michael Khoo, SC argued very forcefully that the court below erred in taking into account matters that were not in the statement of facts. Counsel also argued that the judge below was wrong to have treated this case as if it were a s 9(1) charge when it was not. Section 9 provides for enhanced punishment in circumstances as follows:

9-(1) Where access to any protected computer is obtained in the course of the commission of an offence under section 3, 5, 6 or 7, the person convicted of such an offence shall, in lieu of the punishment prescribed in those sections, be liable to a fine not exceeding $100,000 or to imprisonment for a term not exceeding 20 years or to both.

(2) For the purposes of subsection (1), a computer shall be treated as a "protected computer" if the person committing the offence knew, or ought reasonably to have known, that the computer or program or data is used directly in connection with or necessary for –

(a) the security, defence or international relations of Singapore;

(b) the existence or identity of a confidential source of information relating to the enforcement of a criminal law;

(c) the provision of services directly related to communications infrastructure, banking and financial services, public utilities, public transportation or public key infrastructure; or

(d) the protection of public safety including systems related to essential emergency services such as police, civil defence and medical services.

(3) For the purposes of any prosecution under this section, it shall be presumed, until the contrary is proved, that the accused has the requisite knowledge referred to in subsection (2) if there is, in respect of the computer, program or data, an electronic or other warning exhibited to the accused stating that unauthorised access to that computer, program or data attracts an enhanced penalty under this section.

2 Mr Khoo submitted that when an accused person had pleaded guilty, the sentencing court cannot take into account facts not set out in the Statement of Facts. Counsel very helpfully traced the history of the use of the Statement of Facts through cases cited in *Criminal Procedure*, Tan Yock Lin, Vol 2 page XV 149-222. It is not necessary to discuss these cases in detail. I accept that the Statement of Facts stand as admitted evidence. So, just as a trial judge cannot take cognizance of any fact not proved or admitted in evidence in trial, except those that she might take judicial notice of, she may not take into account facts not found in the Statement of Facts except those that must be reasonably inferred to make sense of the text as a whole. In this case, Mr Khoo submitted that the prosecution accepted that the data copied by the appellant was commercially sensitive and not militarily sensitive. Referring to paragraph 11 of the Statement of Facts, Mr Khoo said that the DPP's submission to the trial judge that the information copied was militarily sensitive, was wrong; and that

that submission probably misled the judge. The relevant passage from paragraph 11 of the Statement of Facts reads as follows, "The above information had been compiled by DSTA from the suppliers' RFI [Request for information] submissions and thus was commercial in confidence." It may be pedantic to argue whether this meant that the information was not therefore "militarily sensitive". Arguments of such a nature only go to show that the statement in question was ambiguous and the court might resolve the dispute in favour of the accused since the burden was on the prosecution to prove its case clearly before the court. I am of the opinion that counsel's argument does not help the appellant. I accept that the facts show the information to be "commercial in confidence", a phrase that was slightly awkward, but conveyed the meaning that the subject matter was a commercial nature in the sense that it related to a purchase of a product by the DSTA from its contractors. It was not entirely devoid of military significance. The fact that it was a rack for munitions storage itself showed that it was a military article. It seems to me that the judge below would not be wrong to take into account the significance of the information to military security. To a layperson, a rack is just a rack. A rack for munitions, its dimensions, price, and even the name of its producer may be valuable information to military observers. That no more serious consequences flowed from the appellant's act could thus be taken into consideration in ameliorating the seriousness of the offence in this case.

3 Mr Khoo's second major argument was based on the submission that the judge erred in imposing a custodial sentence when she did not do so in some recent cases involving the copying of data by the employees of a bank. In those cases, the accused persons were charged (one of them had pleaded guilty to 22 charges out of the 253 charges she was charged with) under s 3(1) read with s 9(1) of the CMA, and yet the same judge did not impose a custodial sentence. See *PP v Low Siok Liang* (DAC 003979/2008 to 004000/2008). Counsel also submitted that with regard to an offence under s 3(1) without s 9(1), the CMA permits the offence to be compounded. Counsel argued that the seriousness of the offence should be considered in the light of these factors. There are many theories of punishment and even more principles concerning the sentencing of offenders. When one considers the range of offences and the punishment prescribed for them he can justifiably conclude that the sentencing of an offender is neither an art nor a science. It is judgment. It calls into play, the sentencing court's understanding of punishment, sentencing principles, and the facts of the case. Facts include, of course, the context of the case and the mitigating and aggravating factors if any. But it is judgment that determines the length and measure of the punishment to be inflicted on the convicted accused. Sometimes that judgment will reflect a measure of public outrage, and sometimes a softer sentiment. Hence, unless the trial judge had clearly erred in law, her appreciation of all the factors necessary for the determination of her discretion as to the sentence should not be overturned unless the sentence imposed was manifestly inadequate or manifestly excessive. Counsel cited the following passage in paragraph 32 of the lower court's ground of decision in support of the contention that the judge below had wrongly taken s 9(1) into consideration:

> 32 Furthermore, aside from the sensitivity of the information copied, the seriousness of the offence was also deepened by the context and circumstances. The agency that was the victim of the unauthorised access is a public agency tasked with defence-related matters. **Although the prosecution did not invoke section 9 of the Act to deem the computer in question a protected computer with a heavier prescribed punishment, the context was clearly one that involved the potential for public harm through undermining of the confidentiality and secrecy of defence-related matters**. That interest required a strong response. (emphasis added) *sic*

I do not get the same impression from that passage as counsel. On the contrary, I am of the view that the passage indicated that the court below was being mindful that this was not a s 9(1) case, and wanted to make it clear that although the sentence she was imposing was not under s 9(1), the punishment should include a jail sentence, but keeping the overall punishment within the range

permitted under s 3(1).

4 The only question remaining was whether the sentence imposed was manifestly excessive. Mr Khoo reiterated the mitigating factors that the offence was not premeditated but committed "on the spur of the moment"; that it was not an instance of computer "hacking"; that the appellant was a respectable businessman whose position in the company would surely suffer from an imprisonment, and submitted that the maximum fine imposed was harsh enough. He submitted that it was excessive to impose a three week jail sentence in addition to the fine. The offence carried a maximum fine of $5,000 or a term of imprisonment up to two years, or both fine and imprisonment. It seemed that the judge below felt that an imprisonment sentence would better reflect the gravity of the offence in the circumstances of this case. It seemed also that given the mitigating factors that counsel advanced on the appellant's behalf in the proceedings below, the judge did not intend to inflict a long sentence. The sentence so imposed was thus appropriate and fair.

5 For the reasons above, this appeal is dismissed.