Public Prosecutor *v* Muhammad Nuzaihan bin Kamal Luddin
[1999] 3 SLR(R) 653; [1999] SGHC 275

Case Number : Magistrate's Appeal No 168 of 1999

Decision Date : 19 October 1999

Tribunal/Court : High Court

Coram : Yong Pung How CJ

Counsel Name(s) : David Lim Jit Hee (Deputy Public Prosecutor) for the appellant; Ravinderpal Singh (Arthur Loke, Bernard Rada & Lee) for the respondent.

Parties : Public Prosecutor — Muhammad Nuzaihan bin Kamal Luddin

Criminal Law – Computer crimes – Unauthorised access to computer networks and modification of content – Sections 3(1), 5(1), 6(1)(a) *Computer Misuse Act (Cap 50A, 1994 Rev Ed)*

Criminal Procedure and Sentencing – Sentencing – Computer crimes – General deterrence versus individual deterrence – Computer Misuse Act (Cap 50A, 1994 Rev Ed)

Criminal Procedure and Sentencing – Sentencing – Whether accused's state of mind relevant to finding of guilt – Whether lack of tangible damage caused to victim companies could be mitigating factor – Sections 3(1), 5(1), 6(1)(a) *Computer Misuse Act (Cap 50A, 1994 Rev Ed)*

Criminal Procedure and Sentencing – Sentencing – Youthful offender – Whether probation order appropriate given nature of offences – Accused committing offences from home – Accused showing persistent course of conduct with felonious intent – Section 5(1) Probation of Offenders Act (Cap 252, 1985 Rev Ed)

Facts

The respondent hacked into one of the proxy servers in the network of Swiftech Automation Pte Ltd, secured unauthorised access to computer files contained in the server and used the server to gain access to the Internet Relay Chat. The respondent also hacked into the File Transfer Protocol server of Singapore Cable Vision Ltd which had earlier rejected his application for an Internet account. For these offences, three charges were preferred against the respondent under the Computer Misuse Act (Cap 50A, 1994 Rev Ed) (the "CMA") to which he pleaded guilty. Fifteen similar charges were taken into consideration for the purposes of sentencing.

The district judge ordered the respondent to undergo 30 months' probation. The Prosecution appealed on the grounds that (a) the judge's finding of fact that the respondent's intention was merely to check for vulnerabilities in computer networks was erroneous; (b) the judge did not attach sufficient weight to the active steps taken by the respondent to conceal his criminal actions; (c) the judge failed to consider the obvious inconvenience caused by the respondent's actions, the time and expense involved in tracing and apprehending him and the inherent damage which computer-related crimes caused to the national interest and public confidence; and (d) the judge should not have given consideration to the fact that the affected computers were not "protected computers" under the CMA.

Held, allowing the appeal and quashing the order for probation:

(1) Although probation was more relevant for young offenders because of the greater chances of rehabilitation compared with adults, s 5(1) of the Probation of Offenders Act (Cap 252, 1985 Rev Ed) made it clear that probation was never granted as of right. Even in the case of juvenile offenders, the court had to take into account all the circumstances of the case, including the nature of the offence and the offender's character: at [16].

(2) Probation orders were rehabilitative in nature and premised on the offender staying at home and off the streets. However, a majority of computer-related crimes were committed at home, as in this case. Public interest required that offenders such as the respondent be put away in a place where they had no access to computers: at [17] and [18].

(3) The district judge erred in finding that the respondent did not possess any criminal intent when committing the offences. The facts showed that he had made a conscious decision to use his hacking skills to serve his own purposes. He took steps to avoid detection and publicly boasted of his feats. For such offences, the courts might have to apply principles of strict liability so that the offender's state of mind was irrelevant to a finding of guilt. Furthermore, the respondent admitted to 15 other offences of a similar nature. This demonstrated a persistent course of conduct and a felonious intent on his part: at [19] and [24].

(4) In certain instances, considerations of general deterrence took precedence over individual or specific deterrence. Cyber-crimes undermined public and international confidence in Singapore's computer systems and compromised Singapore's efforts to position itself as a global e-commerce hub. Besides deterring the respondent from repeating his actions, there was also a need to deter other like-minded individuals. This would give effect to Parliament's express intention that all computer crimes would be dealt with severely in Singapore: at [20] and [21].

(5) The absence of tangible damage caused to the victim companies meant that the charges against the respondent were brought under more lenient provisions of the CMA. Therefore the fact that no damage was caused could not be a mitigating factor. In any event, his offences were conduct crimes for which liability was not dependent on the occurrence of a prohibited result: at [22].

(6) The fact that the respondent was unrepresented in the court below was irrelevant. His decision not to exercise his constitutional right to consult and be defended by a legal practitioner of his choice could not be used as a mitigating factor to the prejudice of the State: at [25].

(7) In the result, the probation order was wrong in principle and was substituted with a sentence of imprisonment of two months on each of the three charges, with the sentence of imprisonment on the first two charges to run consecutively: at [26].

Case(s) referred to

PP v Tan Fook Sum [1999] 1 SLR(R) 1022; [1999] 2 SLR 523 (refd)

Tan Koon Swan v PP [1985–1986] SLR(R) 976; [1986] SLR 126 (refd)

Legislation referred to

Computer Misuse Act 1993 (Act 19 of 1993) ss 3(1), 5(1), 6(1)(*a*) (consd)

Constitution of the Republic of Singapore (1985 Rev Ed) Art 9(3)

Criminal Procedure Code (Cap 68, 1985 Rev Ed) s 18

Probation of Offenders Act (Cap 252, 1985 Rev Ed) s 5(1) (consd)

19 October 1999

Yong Pung How CJ:

1 The respondent was charged with and pleaded guilty in the District Court to three charges under ss 3(1), 5(1) and 6(1)(*a*) of the Computer Misuse Act (Cap 50A, 1993 Ed) ("the CMA"), for unauthorised access to computer materials, unauthorised modification of the contents of a computer and unauthorised access to a computer service respectively. Fifteen other charges under the same provisions of the CMA were taken into consideration for the purposes of sentencing. After calling for a pre-sentence report, the district judge ordered the respondent to undergo six months of intensive probation and 24 months of supervised probation with the following added conditions:

(a) a time restriction from 10pm to 6 am;

(b) the performance of 200 hours of community service; and

(c) a requirement for the respondent's parents to sign a bond of $5,000 for his good behaviour.

The Prosecution appealed against the sentence imposed by the district judge. After hearing arguments from both sides, I allowed the Prosecution's appeal and quashed the order for probation made by the district judge, substituting it with a term of imprisonment of two months on each of the three charges. I now give my reasons.

The charges

2 The respondent was charged as follows:

DAC 20070/1999

You, Muhammad Nuzaihan bin Kamal Luddin, m/17 yrs NRIC No S8140891B, are charged that you, in the month of July 1998, in Singapore, did knowingly cause the computer of Swiftech Automation Pte Ltd, namely, the server Cloud4, to perform a function, to wit, processing and granting access request, for the purpose of securing access without the authority of the system administrator, to the computer files held in the said computer and you have thereby committed an offence punishable under s 3(1) of the Computer Misuse Act (Cap 50A).

DAC 20076/1999

You, Muhammad Nuzaihan bin Kamal Luddin, m/17 yrs NRIC No S8140891B, are charged that you, in the month of July 1998, in Singapore, did knowingly secure access without authority to the computer of Swiftech Automation Pte Ltd, namely, the server Cloud4, for the purpose of obtaining a computer service, to wit, you did utilise port 31337 of the said computer to gain access to the Internet Relay Chat, and you have thereby committed an offence punishable under s 6(1)(a) of the Computer Misuse Act (Cap 50A).

DAC 20082/99

> You, Muhammad Nuzaihan bin Kamal Luddin, m/17 yrs NRIC No S8140891B, are charged that you, in the month of July 1998, in Singapore, did knowingly cause an unauthorised modification to the contents of the computer of Singapore Cable Vision Ltd, namely the server Brahms, to wit, by modifying the content of the computer file, namely, 'inetd.conf', without the authority of the system administrator, and you have thereby committed an offence punishable under s 5(1) of the Computer Misuse Act (Cap 50A).

The facts

3 These were contained in the statement of facts read out in the court below to which the respondent admitted unreservedly without qualification. They were as follows.

4 On 7 July 1998, one Walter Klomp, the system manager of Swiftech Automation Pte Ltd ("Swiftech") lodged a police report with the Criminal Investigation Department ("CID"), informing them that someone had gained unauthorised access to Swiftech's proxy server and had modified its contents. Swiftech is a value-added service provider for SingNet, from which it is sublicensed to operate a full range of internet services ranging from personal dial-ups, network dial-ups, internet integration and network integration *etc*. It operates from its own web servers, proxy servers and modem pools.

5 On 4 August 1998, the respondent was arrested at his home by a team of police officers from the Computer Crime Branch of the CID. Investigations revealed that sometime between October and December 1997, during the year-end school vacation, the respondent started to read up extensively on computer security and soon developed an interest in the subject. In time, he discovered that certain flaws existed in Linux operating systems, in consequence of which he began to learn about the ways of checking for vulnerabilities in computer networks. Sometime in June 1998, the respondent decided to "hack" into various foreign servers, believing that such conduct would not be easily detected or traced by the relevant system administrators who were mostly located abroad. He managed to hack into four foreign sites successfully without being detected by their system administrators. As a result of this "achievement", the respondent became more confident about hacking and subsequently decided to test his skills on local servers.

Facts relating to DAC 20070/1999

6 Sometime in June 1998, the respondent detected certain vulnerabilities in some of the servers comprised in Swiftech's network whereupon he decided to hack into one of the proxy servers of the network, namely "Cloud4", as its role was of the least importance and consequently any intrusion would be less likely to be detected by the system administrator. In July 1998, the respondent downloaded an exploit known as "ROTShB" (Riders Of The Short Bus) from the Internet. He compiled the program codes of this exploit into a program which he executed on Swiftech's network, via the server "Cloud4". The execution of the program caused the server "Cloud4" to process and grant access request to the respondent, allowing him to secure access to the computer files contained in "Cloud4". All the accesses made by the respondent to the computer files of "Cloud4" were done without the authority of Swiftech's system administrator.

Facts relating to DAC 20076/1999

7 After gaining root access to the server "Cloud4" of Swiftech, the respondent executed a program known as "bounce" which he uploaded to "Cloud4". Upon execution of "bounce", the port 31337 of the server "Cloud4" was automatically reconfigured to allow the respondent to utilise the server to gain access to the Internet Relay Chat ("IRC"). The respondent had thus successfully created a user account for himself in the server "Cloud4", which account he made use of to connect to the IRC. While on the IRC, the respondent indicated to the other users on the channel that he was able to compromise a server which ran on a Linux operating system.

Facts relating to DAC 20082/1999

8 At or around the same time that the respondent did the above acts, he also hacked into the File Transfer Protocol ("FTP") server "Brahms" of Singapore Cable Vision Ltd ("SCV"). The respondent had earlier applied to SCV for an internet account but was rejected as the cable modem service was not then available to his estate. As such, he decided to gain unauthorised access to the server "Brahms" in order to make use of the cable network's high-speed link to download files from the Internet. Upon gaining access to "Brahms", the respondent amended several files in the server and later configured a backdoor known as "nightman" at port 22 of the server which allowed him to access the server "Brahms" in future without having to hack into the system again. He would remove his trails from the server "Brahms" by deleting the system logs every time before logging out from the server.

9 No tangible damage was caused to the computer systems of both Swiftech and SCV.

10 In mitigation, the respondent, who was unrepresented in the court below, said that he was remorseful. He also informed the court that he would be sitting for his GCE "O" Level examinations at the end of the year and pleaded for a second chance.

The decision below

11 In ordering the respondent to be placed on 30 months' probation, the district judge took into account what he considered to be the mitigating factors present. These were the respondent's early plea of guilt and concomitant show of remorse, his youthful age of 17, his lack of antecedents and the fact that he was unrepresented in the court below. Despite noting that offences under the CMA were serious offences necessitating the imposition of deterrent sentences for the protection of the public, the district judge was nevertheless of the view that the degree of severity varied for different offences under the CMA. In particular, he was influenced by the fact that the computers and network systems which the respondent had hacked into in this case were not "protected computers or systems" under the CMA. As such, neither national security nor public security had been breached and no tangible damage was caused by the respondent's actions. In addition, the district judge also found that the respondent's intention all along was only to check for vulnerabilities in computer networks. In light of the above, a custodial sentence was felt to be inappropriate. The district judge concluded that what the respondent needed was close supervision by his parents and the proper authorities to lead him along the right path.

The appeal

12 The Prosecution contended that the district judge had erred in fact and in law in coming to his decision to impose a probation order on the respondent. This was manifestly inadequate given the circumstances of the case.

13 Firstly, the Prosecution submitted that the finding of fact that the respondent's intention was merely to check for vulnerabilities in computer networks was erroneous as the statement of facts showed clearly that the respondent's intention throughout was both self-serving and criminal. Secondly, the district judge did not attach sufficient weight to the fact that the respondent had taken active steps to conceal his criminal acts in order to avoid detection. Such conduct, the Prosecution contended, clearly demonstrated that the respondent was fully aware of the criminality of his actions. Thirdly, the district judge also failed to appreciate the true distinction between tangible and intangible damage in cases of computer-related crimes, thereby omitting to consider the obvious inconvenience caused to the companies affected by the respondent's actions, the time and expense incurred by the police and the victims' staff to trace and apprehend the respondent and to establish the extent of his intrusion into their systems, the inherent damage which computer-related crimes cause to the national interest and the effect which such conduct has on the public confidence, particularly in the context of Singapore's efforts to position itself as an intelligent island. Finally, the district judge had erred in wrongly giving consideration to the fact that the computers hacked into were not "protected computers" under the CMA.

14 In response, counsel for the respondent submitted that his client did not commit the offences out of greed nor did he at any time harbour any evil or sinister intent. He was not a gang member and the offence in question was not violent in nature. Counsel also urged me to bear in mind that rehabilitation was the dominant consideration where the offender is under 21 years of age as the chances of reforming such offenders into law-abiding adults are better. Compassion is often shown to young offenders on the assumption that the young "don't know any better" and may not have had enough experience to realise the full consequences of their actions. Finally, counsel stressed that probation had previously been ordered in cases involving far more serious crimes like culpable homicide.

Principles of sentencing

15 Section 5(1) of the Probation of Offenders Act (Cap 252, 1985 Rev Ed) ("the Act") provides as follows:

> Probation
>
> 5(1) Where a court by or before which a person is convicted of an offence (not being an offence the sentence for which is fixed by law) is of the opinion that *having regard to the circumstances, including the nature of the offence and the character of the offender, it is expedient to do so*, the court may, instead of sentencing him, make a probation order, that is to say, an order requiring him to be under the supervision of a probation officer or a volunteer probation officer for a period to be specified in the order of not less than 6 months nor more than 3 years. [emphasis added]

16 Probation under the Act is intended to be used to avoid the sending of offenders of not very serious offences to jail, where they may associate with hardened criminals, who may lead them further along the path of crime. The Act recognises that many of these crimes are committed through ignorance or inadvertence or due to the bad influence of others. The offenders, but for such lapses, might be expected to be good citizens in which case a term of imprisonment might have the opposite effect to what is intended to be served by the imposition of the sentence. The traditional and broad rationale of probation therefore has always been to wean offenders away from a lifetime career in crime and to reform and rehabilitate them into self-reliant and useful citizens. In the case of youthful criminals, the chances of effective rehabilitation are greater than in the case of adults, making the possible use of probation more relevant where young offenders are concerned. Nevertheless, the above-italicised portions of s 5(1) of the Act make it clear that probation is never granted as of right, even in the case of juvenile offenders. In deciding whether or not probation is the appropriate sentence in each case, the court still has to take into account all the circumstances of the case, including the nature of the offence and the character of the offender.

17 Having heard the submissions of both sides, I came to the view that probation is not suitable for offences of the type with which the respondent was charged under the CMA. Probation orders based on the simple concept of rehabilitation, with the usual restrictions on the offender to remain at home between dusk and dawn are not realistic solutions for these new crimes, which more often than not are committed by the offenders from home. Hitherto probation orders have been granted to what, for lack of a better term, might be called "amateur offenders", in respect of traditional "blue-collar" Penal Code offences. The rationale for this was to keep these youngsters off the streets in order to prevent them from mixing with the wrong company outside and from engaging in gang activities or other harmful and self-detrimental exploits. For probation to work, a not inconsiderable amount of responsibility is placed on the parents of offenders to ensure that their children comply with the time restrictions imposed in order that these teenagers stay at home and out of trouble with the law.

18 The inherent nature of offences under the CMA makes probation orders ineffective, as keeping the offender at home in such cases does not guarantee that the offender will not repeat his actions. There is no doubt that a majority of these computer-related crimes are committed at home, and certainly this was the case here. That the parents have failed to avert the commission of these offences in the first place, despite the fact that they were committed at home, fortifies the view that responsibility for the offender's future behaviour can

no longer be left in the hands of his parents. The public interest requires that offenders such as the respondent be put away in a place where access to the major instrument of his crime is not available to him in order that he is not afforded any opportunity to re-offend.

19 With respect to the district judge, I disagreed with his finding of fact that the respondent's only intention in accessing the various networks was to check for vulnerabilities in them. I agreed with the Prosecution that the statement of facts revealed clearly that the respondent had made a conscious decision to use his hacking skills on local servers after having gained confidence from his success at hacking into foreign sites. He not only gained unauthorised access to the local servers, but also went further and modified the programs in the server "Brahms" which action enabled him to access the server in future without having to hack into the system again. Thereafter, he made use of SCV's computer services for his own purposes and even had the presence of mind to obliterate all traces of his intrusions so as to avoid detection. It is pertinent that the respondent had hacked into the server "Brahms" only after SCV had rejected his application for cable subscription. The obvious inference to be drawn from this was that the respondent, being dissatisfied with SCV's response, deliberately set out to get around the problem by utilising illegal means. His arrogance was also evident in the fact that he had proudly proclaimed to the other IRC users that he was able to compromise a server running on the Linux operating system. It was not correct therefore that he did not possess any criminal intent when committing the offences for which he was charged. A teenager of 16 or 17 years who commits such offences must be intelligent enough to know that it is wrong and dishonest of him to do so and the punishment for these offences must be brought home to him directly. In any case, this is an area of activity in which there can be more teenagers involved than adults. As a result, when offences such as these are committed, the courts may well have to apply the principles of strict liability so that the offender's state of mind is irrelevant to a finding of guilt.

20 In addition to the need to deter the respondent from repeating his actions, I was also mindful of the need to deter other like-minded individuals from doing the same. In this respect, it is relevant to repeat the pronouncement I made in *PP v Tan Fook Sum* [1999] 1 SLR(R) 1022 that considerations of general deterrence must in certain instances take precedence over those of specific or individual deterrence, particularly where the public interest demands that this be so. In my view, such anti-social conduct on the part of the respondent not only undermines public and international confidence in the commercial integrity and viability of our computer systems, it also gravely compromises Singapore's efforts to position itself as a global e-commerce hub. The potential for which these cyber-crimes have in undermining Singapore's burgeoning information technology ("IT") industry cannot be ignored. IT security is a major consideration which many foreign companies take into account before deciding whether or not to develop and invest in the local IT sector.

21 Even though the respondent's acts took place just before the coming into effect of the recent amendments to the CMA on 1 August 1998, the policy considerations highlighted during the Parliamentary debates relating to these amendments remain pertinent and are similarly applicable to the case at hand. In particular, during the second reading of the Computer Misuse (Amendment) Bill on 30 June 1998, the Minister noted at column 392 that:

> … crimes committed through the electronic medium and through use of computers are difficult to detect but they are just as serious as traditional crimes and we must equally protect our population against such crimes. To ensure that Singapore remains an attractive place for investors and businesses to operate effectively and securely, computer crimes must be treated as seriously as other criminal offences.

In the result, I had no hesitation that a deterrent sentence had to be meted out on the respondent in order to give effect to Parliament's express intention that all computer crimes will be dealt with severely in Singapore.

22 Counsel for the respondent urged the court to give weight to the fact that no tangible damage was caused to the servers of both Swiftech and SCV as a result of the respondent's actions. In my view, the absence of tangible damage caused to the victim companies was counterbalanced by the immeasurable inconvenience which they had to put up with in establishing the extent of the respondent's intrusion into their systems. At the same time, there is no telling the amount of resources which the companies had to expend to reinstate their systems. Much time and expense was also incurred by the CID in tracing and apprehending the respondent and thereafter in investigating into the extent of his criminal activity. In any case, the offences for which the

respondent was charged are conduct-crimes, liability for which is not dependent upon the occurrence of a prohibited result. Rather, criminal liability is imposed simply because the offender has done something which is prohibited by law. If damage had indeed been caused to the computer systems of the victim companies, different provisions in the CMA carrying heavier punishments would have been applicable. The fact that no damage was caused therefore cannot be used as a mitigating factor where the charges are brought under the already more lenient provisions of the CMA.

23 I also took issue with the district judge's finding that mitigating value should be attached to the fact that the computers intruded into were not "protected computers" under the CMA and that neither national nor public security was breached in this case. In my opinion, there was no question that the respondent escaped facing a heavier punishment in view of the fact that the servers of Swiftech and SCV did not fall within the definition of "protected computers" under the CMA. However, the fact remained that the offences committed by the respondent were in themselves serious enough for me to take a stern view of the matter. In any case, that the respondent did not commit a more serious offence under the CMA is not ground for showing him leniency when sentencing him for a separate offence for which a distinct set of punishment is prescribed by law.

24 It was also relevant that the offences in question were not one-off isolated incidents committed out of boredom or curiosity amidst the throes of harmless youthful rebellion. Rather, the respondent had pleaded guilty to three separate offences and had in addition admitted to 15 other offences of a similar nature. I was thus called upon to take into account a persistent course of conduct which clearly evidenced a felonious intent on the part of the respondent.

25 Finally, the fact that the respondent was unrepresented in the court below was irrelevant. Article 9(3) of the Constitution of the Republic of Singapore states unequivocally that every accused person has the right to consult and be defended by a legal practitioner of his choice. As such, the fact that the respondent chose not to exercise a right given to him by the State cannot now be used as a mitigating factor in his favour to the prejudice of the State.

The appropriate sentence

26 Policy considerations, the far-reaching effects which the offences have on the public interest if their pervasion is not halted at an early stage, and the seriousness with which Parliament views cyber-crime, all mandated the imposition of a custodial sentence. In determining the proper length of that sentence, I kept in mind the respondent's youth, the generally favourable report given by his form teacher regarding his conduct and the fact that he was a first offender. Having considered all the circumstances of the case, I allowed the Prosecution's appeal and quashed the probation order made by the district judge on the ground that the district judge had passed a sentence which was wrong in principle (see *Tan Koon Swan v PP* [1985–1986] SLR(R) 976) in that it failed to take into account the need for deterrence and the fact that probation was not suitable for offences of the type with which the respondent was charged. I then substituted the lower court's order with a sentence of imprisonment of two months on each of the three charges against the respondent. In view of the mandatory requirement laid down in s 18 of the Criminal Procedure Code (Cap 68), I ordered that the sentence of imprisonment on the first two charges should run consecutively while that on the third charge should run concurrently with those on the first two charges, making a total of four months' imprisonment.

27 I recognise that the respondent is an intelligent and resourceful young man whose true talent and potential, when harnessed under the right conditions, can be of immense value to the country. It is hoped therefore that the experience of life in prison will instil in him a sense of maturity and responsibility, and teach him to put his computing skills to legitimate use upon his release, thus enabling him to contribute usefully to society.

Headnoted by Linda Esther Foo.

BACK TO TOP