

The year 2000 bug: not just an “IT” problem

Jeanetha Brink
Pretoria Bar

Dear Pentiamus,

Are you still working on the Y zero K problem? This change from BC to AD is giving us a lot of headaches and we haven't much time left. I don't know how people will cope with working the wrong way around ... We called in Consultus, but he simply said that continuing downwards using minus BC won't work and as usual charged a fortune for doing nothing useful. Surely we shall not have to throw out all our hardware and start again? He checked out all our hardware and noted that at least our abacuses and sun dials will still work okay as they are not date dependent. However, he says, we may pick up a problem with prediction equipment in the seers department. Macrohard will make yet another fortune out of this, I suppose.

Computorius.

(Extracts from this article was taken from the Internet (atuson@nwpg.org.za) titled “Y0K”, apparently translated from a Latin scroll dated about 2BC.)

Good for a giggle? Yes, maybe because there's a ring of truth to it. The last year of the century has many of us excited in anticipation of the Millennium, but let's not forget that we are facing a non-negotiable deadline on 31 December 1999. This is the date causing headaches to those working 'round the clock to fix the problem on time. It also seems that generally attitudes are changing from ignorance to awareness as the general public realises that it's much more than a computer problem: it certainly entails much more than having your PC tested for Year 2000 compliancy.

So what's all this about? It's about a computer software monster created some 40 years ago when computers were, compared to the current technology, not nearly as advanced as they are at present. One of the drawbacks was that they had very little memory and storage space. In addition, this storage was very costly. In order to save both space and costs, the field for the year-date was designed to have two non-variable digits, which were the first two, i.e. the “19” in, for example, “1999”. The problem which now arises, is the following: unless the software is corrected, most business application software programs (mainframe, client/server

and personal computer) will, on 1 January 2000, recognize the year as “00” and may assume that the year is “1900”. This could either force the computer to shut down or lead to incorrect calculations: for example, a financial spread sheet or projection showing the financial trend for the 1999-2000 period could be projected running backwards rather than forwards if the computer should interpret the date as 1999-1900¹. This “correction” of the computer software is what is generally referred to as: “obtaining Year 2000 compliancy”, in other words, the ability of the software to be able to correctly process the date change from 1999 to 2000.

As modern society became increasingly dependent on computers, and, as the need and use for computers grew, networks were developed to allow computers to communicate with one another. The process can be referred to as “systems integration”: multiple complex systems emerged to form highly interdependent meta-systems. This creates a particularly threatening situation in that enhanced integration of such systems increases the risk of “collateral damage” to systems: this refers to damage caused to systems not directly affected, but damaged due to their reliance on information from damaged systems.² The data thus transferred to the different computers in the system, which is

“contaminated data”, could have the same effect as a computer virus would have since it “infects” the whole system. The result could then be that, even though a system had been made “year 2000 compliant”, it could still fail or malfunction because of the contaminated data having been conveyed throughout the system. To name but a few of the functions which could be affected, reference can be made to computerized tasks requiring date dependent arithmetic calculations and sorting and sequencing date functions.³ This could, for example, include bank statements, pension payments, bond calculations and statements, invoices etc.

Embedded chips

Are you interested yet? There's more: the “dark horse” is the problem pertaining to “embedded chips”. These are microprocessors (small computers) that are found in single non-computer devices.⁴ These could include cellular phones, microwave ovens, automated systems such as elevators, medical equipment, fire alarm and security systems to name but a few. These chips regulate the basic functioning of these machines.⁵ Many of these embedded chips contain date references to enable them to perform certain basic tasks essential to their proper functioning.⁶ The problem is that these chips need to be replaced to ensure that the device they regulate will not stop functioning. This seems an impossible task since there are billions of chips installed in various devices: it is estimated that in 1993 alone, over 2 billion micro chips were sold.⁷ In addition, special knowledge of embedded programming languages is required to change these systems.⁸

It should be clear that the vastness of the problem can hardly be underestimated. Apart from the obvious implications of businesses not being able to operate normally, it should be clear that our daily lives will surely be affected. From traffic lights to banks, from household appliances to necessary commodities such as water and electricity, almost every system as we know it is at risk. Bear in mind the impact on the economy: ING Barings predicts⁹ that the GDP growth might drop by 1,1% as a direct result of Year 2000 disruptions.

Legal implications

The shut down of computer systems, or ever the malfunctioning of computers and compu-

* *Information Technology*

ter-integrated systems, can of course lead to businesses being seriously hampered in their normal business activities. This will lead to financial loss for the business, be it directly as a result of not being able to supply the normal product or service, or because of losses incurred in third-party relationships. A diversity of legal relationships will be involved and extensive litigation is being predicted. In this instance an example can be put to use to illustrate the point: *The electricity is interrupted in Pretoria for 2 days. A chain store is, apart from not being able to conduct its day-to-day business, subject to burglaries/looting since the security system is not working. It submits a claim to the insurance company, which denies responsibility for Y2K related damages.* It should be mentioned that insurers are advising business clients that Y2K-related damages will not ordinarily be entertained unless certain remedial steps had been taken. However, should insurance-related claims be submitted and denied, a business might consider litigating to recover its damages?

Existing contractual relationships may also lead to litigation should grounds be found to exist to found a claim for breach of contract. The more obvious relationships are those existing between suppliers and developers of software with either individuals or companies; it can also be extended to per-

sonnel-related agreements, e.g. contractors employed for Y2K remedying assignments. It will, for example, need to be established whether the terms pertaining to maintenance of a computer software system included reference to Y2K related problems. This could prove problematic in an existing agreement which had not been reviewed bearing in mind Y2K anticipated problems. Another example of expected problems could refer to a claim instituted to recover damages where, in order to establish causation, many software-related problems will have to be excluded. Another prediction is the very eminent danger of insolvency. In this regard businesses are advised to establish their risk areas since "bad debts" as a result of Y2K problems, constitute one of the biggest threats.

However, actions instituted to recover damages flowing from delict will probably be more prevalent. Negligence would most often lie in conduct by way of *omission*. Of particular importance is the possible liability of company directors and hospitals. Many systems in hospitals function on computer software and if the result of malfunctioning of such systems or software is not obvious enough, one must bear in mind that hospitals may also suffer from business interruptions. This may for instance increase the risk of non-availability of medication, blood, etc.

One must bear in mind that much of the publication on the subject is highly speculative. According to recent media reports, the Y2K compliancy in South Africa is well on track, and South Africa is rated amongst the top ten countries in the world as regards our Y2K compliancy. This certainly seems very reassuring, and hopefully it will result in much less chaos than is being predicted at present.

Endnotes

- 1 Jinnett, J. 1996. *Legal issues concerning the year 2000 "Millennium Bug"*, <http://www.year2000.com/archive/legalissues.html>, p 1.
- 2 Meagher, E. 1997. *Y2K and our computer dependency*, Westergaard year 2000, p 1.
- 3 *The year 2000 software crisis: management and legal gauntlet of the millennium*, <http://www.year2000.com/archive/brief.html>, p 1
- 4 1997. *Explaining the embedded chip year 2000 problem*, Westergaard year 2000, p 1.
- 5 *Ibid.*, p 1.
- 6 *Ibid.*
- 7 Jinnett, J. 1997. *Testimony*, <http://www.comlinks.com/gov/jin710.htm>, p 2.
- 8 Campbell, E. 1996-1998. *The Millennium bug and you*, <http://www.everything2000.com/comp/fpstory.html>, p 2.
- 9 McLeod, D. "As the time bomb ticks...", *Financial Mail*, 19 February 1999, p 86. 

Aspects of practice • Praktyksbrokkies

John Middleton
Pretoriase Balie

Hierdie bydrae behels die *Suid-Afrikaanse Hofverslae* en die *All South African Law Reports* vir die tydperk 1 Januarie tot die einde Maart 1999 en die *Suid-Afrikaanse Strafregverslae* en *Butterworths Constitutional Law Reports* vir die tydperk 1 Januarie tot einde Februarie 1999.

Constitutional Court: Practice Direction 2

The following Practice Direction was issued by the President of the Constitutional Court on 17.02.1999:

"1 When an application for confirmation of an order of constitutional invalidity or a notice of appeal against such order is lodged with the Registrar in terms of rule 15, or an application for leave to appeal is lodged in terms of

rules 18 or 20, the applicant or appellant shall at the same time provide the Registrar with a note;

- (a) setting out the length of the record, or if the record consists of evidence that has not been transcribed, an estimate of the length of the record and the time required for transcription.
- (b) whether there are any special circumstances that may require a

hearing of more than one day or which might otherwise be relevant to the directions to be given by the President.

- 2 Where documents, including records, which are longer than five pages are lodged with the Registrar, and such documents are recorded on a computer disk, the party lodging the document should where possible also make available to the Registrar a disk containing the file in which the document is contained, or transmit an electronic copy of the document concerned by e-mail in Wordperfect format (5, 6 or 7) to the Registrar at: courtcases@concourt.org.za
- 3 If a disk is made available to the Registrar the file will be copied and the disk will be returned to the party concerned. Where a disk or an electronic copy of a document other than a record is provided, the party need lodge only