Criminal Records in the European Union,

the challenge of large-scale information exchange[1]

by Jan Grijpink[2]

Introduction

This article explores some unintended side-effects of the EU-Counsel's decision to exchange information on criminal convictions within the European Union. In the aftermath of the Belgian-French Fourniret case the European Commission insists on an urgent implementation of the Counsel's decision and announced a Communication to that purpose before the end of 2005. The approach taken here is based on the theory of chain-computerisation, thus taking closer account of the specific problems of large-scale information exchange and cross-border cooperation in law enforcement to prevent cross-border crime or migration of criminals from going unnoticed. Chain-analysis of the necessary information exchange demonstrates that unless we adopt additional precautions the volume of identity fraud in criminal cases involving nationals abroad will increase substantially. This will cause national criminal records to be more often incomplete and incorrect, resulting in wrong decisions, for instance in relation to sensitive appointments like Fourniret's. Abroad, criminals can easily make use of other identities because these cannot effectively be checked by foreign law enforcing authorities. Cross-border identity fraud in criminal cases enables criminals to disperse their crimes over a set of criminal records while keeping their true identities clean. The insights derived from this chain-analysis prove to be essential for a consistent European system of cross-border use of national criminal registers.

Outline of this article

After the introduction of the chain concept and some elements of a suitable chain approach, the challenge of large-scale information exchange in chains is explained. The chain approach is subsequently applied to the European criminal registry to prevent the Fourniret case from happening again. In two steps the interconnected procedures across the European Union are demonstrated to produce this combined effect only if Member States perform cross-border checks on their own citizens in criminal procedures in other member States using forensic biometrics. Next, the special character of chain-computerisation is set out resulting in an explanation of its standard model of large-scale information exchange and its underlying constitutional requirements. Finally, some conclusions are drawn about the chain approach in general and its relevance to the cross-border use of criminal records within the EU.

Chain issues

Barely a day goes by without chain issues making the news. Today's headlines are about football hooliganism, tomorrow's about juvenile delinquency or medical errors caused by faulty data transfer. Topical themes on the subject of chain cooperation include passport biometrics, the citizen service number and mounting identity fraud, for example. These issues always involve the large-scale exchange of information between huge numbers of independent organisations and professionals. They are often confronted with faulty cooperation or direct opposition by the person involved, by a suspect in the criminal law enforcement chain for instance. If something goes systematically wrong with the communication in a chain, so many wrong decisions are taken that the chain becomes discredited. Our ability to tackle social problems is not keeping pace with the development of our society. In a social chain, no single party has the power to compel others to cooperate effectively. We are thus confronted with chain issues that are difficult to resolve. The computerisation of our society does however hold the promise of better-informed chain cooperation. But the gulf between what we are actually doing in the area of large-scale information exchange and what we need to do is getting bigger rather than smaller. In fact, we know precious little about how to bring about the exchange of information at such a huge scale, at least with sufficient guarantees of the data being used lawfully. The goal of the field of study ‘Chain-computerisation in the constitutional state’ is to improve that situation. That is all the more important when we consider that the formation of the EU is leading to the internationalisation of many social chains, with all the complications that entails for the effective, lawful exchange of information.

Chain-computerisation

Our emerging information society increasingly calls for an approach of external communication that takes closer account of the needs and preconditions of chain cooperation. The large-scale exchange of data between autonomous organisations calls for a computerisation approach that is different from what we are used to. We must move away from treating large-scale communication systems as intra-organisational information systems with a somewhat larger group of users. It is for that reason that a distinct scientific basis with its own concepts, theories and methods is needed for the computerisation of social chains. That must give rise to new insights into the causes of the problems we are facing in the development of information infrastructures. In past years the foundation has been laid for tenets of that nature in a series of publications[3], which have now been institutionalised in the form of an endowed chair entitled *Chain-computerisation in the constitutional state*. Within the broad framework of information and computer sciences, *Chain-computerisation in the constitutional state* can be regarded as a sub-discipline in its own right, because it features all of the four characteristics required for that purpose[4]. The social significance of these tenets is found in the notion that new insights can lead to better information strategies for our complex information society. That means more suitable information infrastructures for chain cooperation (covering the entire range from hard to soft infrastructure, from cables up to and including knowledge). Applying the chain-computerisation theory makes it possible to distinguish promising chain projects from the rest, so that essential information infrastructures can be created more quickly. How can we otherwise structurally avoid a future situation in the travel chain in which somebody gets into difficulty in a foreign country because his identity has been misused? Or, without information infrastructures of that nature, how can we immediately establish in the criminal law chain of the future that the suspect is someone other than who he has led the police to believe he is? Or that he is a habitual offender who needs to be tackled in a special way? Which chain communication do we need in the future to prevent new citizens from becoming isolated in our society? There are countless other examples that could be given. In many social chains the number of misses, the so-called ‘chain failure’, is becoming an increasingly serious problem, further reinforced by our diminishing tolerance for poorly functioning social chains.

The ‘chain’ concept and the dominant chain problem

The word ‘chain’ has now been used a few times consecutively. By ‘chain’ is not so much meant the logistics chain that we so often come across in the business community, but a social chain, such as social security, criminal law enforcement or treatment for drug addiction. Those are large-scale processes that yield a social product, such as income support, safety or survival. In a social chain of that nature many hundreds if not thousands of organisations work together without a clear relationship of authority in ever-changing combinations depending on the actual case. But cooperating with other organisations takes a lot of effort, time and money. There must therefore be a cast-iron reason for doing it. An important principle of our ‘chain’ concept is therefore that parties to a chain only cooperate if they are forced to do so by a dominant chain problem. A dominant chain problem is a problem that none of the parties can solve on his own. It is only by effectively cooperating that chain parties can prevent the systematic failure of their own organisation and the entire chain from being discredited. The identity chain, for example, cannot yet prevent your identity from being misused by someone else undetected. Identity fraud as a dominant chain problem in the identity chain forces parties to cooperate and determines the information infrastructure needed for that purpose, in which biometrics will play a central role in the future.

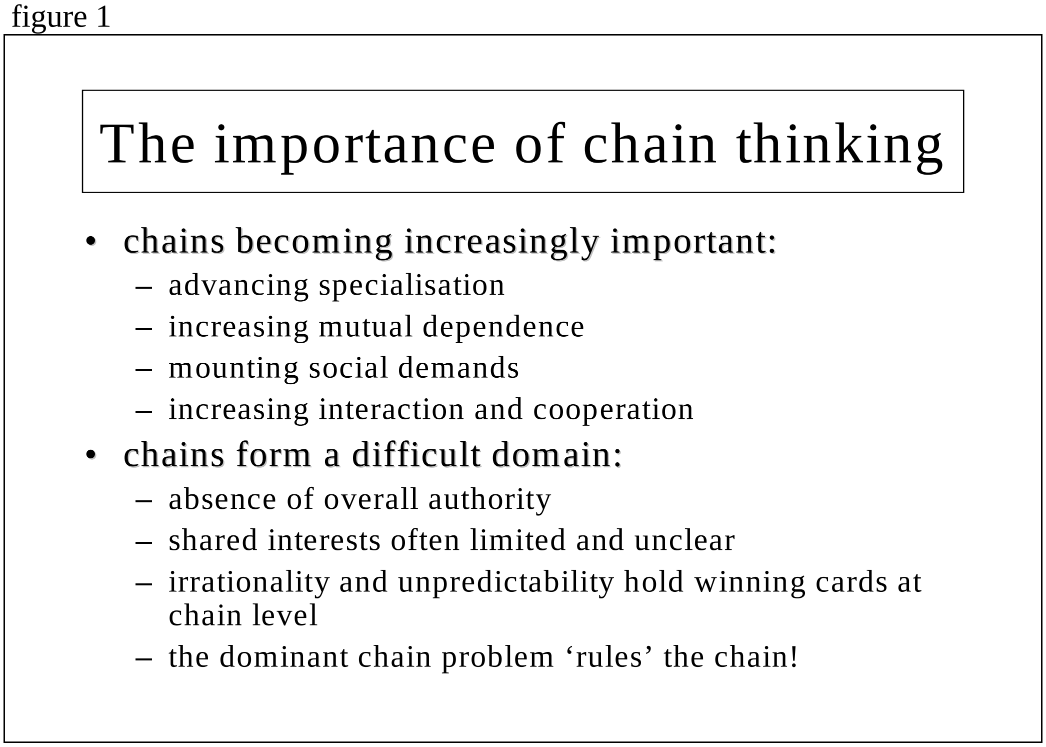
Ten years ago the concept of a ‘chain’ was still a vogue word without any practical significance. These days, we are more aware that each organisation must participate effectively in a large number of different chains. In practice, we find that it is difficult to reconcile the requirements of various chains. If an organisation acts both in the disaster recovery and the criminal law chain, should that organisation participate both in a chain with a geographically-based communication system (*where* is it?) and in a chain with a person-based communication system (*who* is it about?). These very different structures can explain why many organisations have so much trouble with finding a suitable intra-organisational information infrastructure.

Chain thinking and chain laws

Chain thinking is gaining in importance. Figure 1 briefly shows why. Advancing specialisation and mounting social requirements make organisations more and more dependent on each other. But chain cooperation proves to be anything but easy in practice. Because common interests are less pronounced than people think, and also often unclear, the cohesion that is so badly needed can only be provided by a serious dominant chain problem. Only then is there sufficient official and professional support for the large-scale exchange of information. Because of the absence of overall leadership, the chain proves to be a difficult administrative domain, in which processes like cooperation, decision-making and exchanging information proceed differently than *within* organisations. Rationality and expediency are often hard to find at the collective ‘chain level’, and unpredictability is the order of the day. If we leave aside the presupposition of rationality at chain level, we gain a clearer image of laws that play a predominant role at that level. Some of them are shown in figure 2. Only a gradual approach, a modest measure or a selective system has any chance of success. The grander the envisaged solution, the less actual support there will be.

Measures at chain level that exert a strong outside influence on the internal affairs of chain partners come up against a lot of resistance. We know this from the world of international diplomacy, but we rarely apply this insight to chain cooperation.

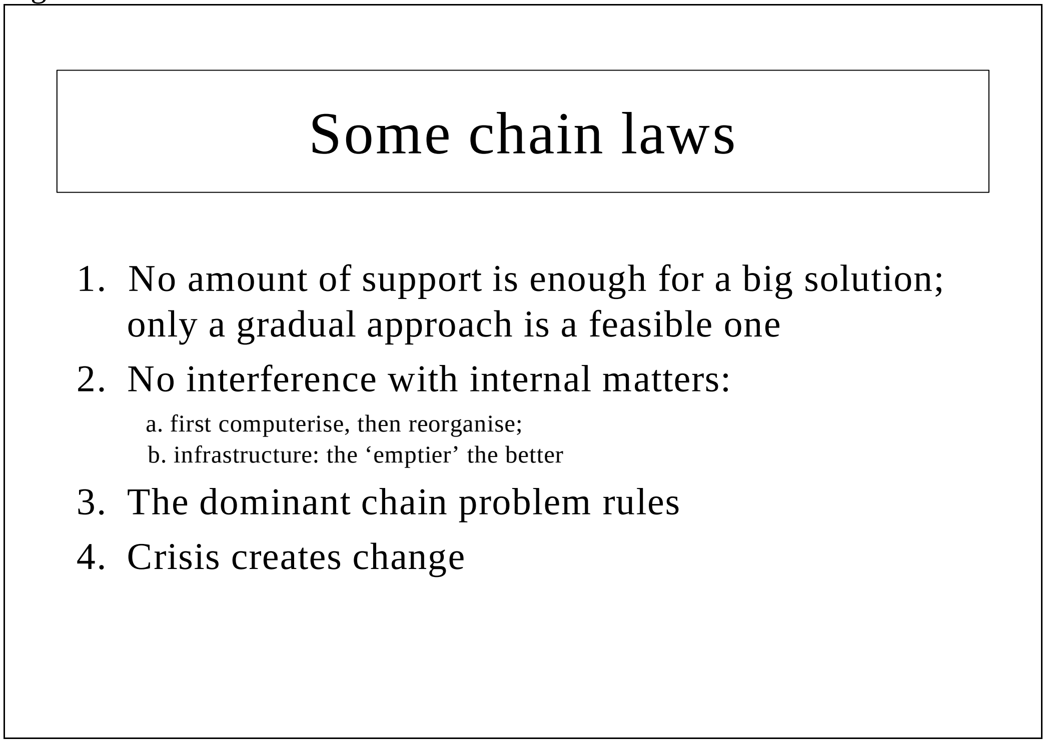
figure 1



The importance of chain thinking

- chains becoming increasingly important:
  - advancing specialisation
  - increasing mutual dependence
  - mounting social demands
  - increasing interaction and cooperation
- chains form a difficult domain:
  - absence of overall authority
  - shared interests often limited and unclear
  - irrationality and unpredictability hold winning cards at chain level
  - the dominant chain problem ‘rules’ the chain!

figure 2



Some chain laws

1. No amount of support is enough for a big solution; only a gradual approach is a feasible one
2. No interference with internal matters:
   a. first computerise, then reorganise;
   b. infrastructure: the ‘emptier’ the better
3. The dominant chain problem rules
4. Crisis creates change

For example, it follows from the rule of ‘mind your own business’ that at chain level, unlike within organisations, computerisation of the essential communication has more chance of success than reorganising or integrating information systems. Nevertheless, we often prefer solutions that reinforce or change responsibility structures or tasks.

Large-scale change processes based on the power of persuasion and good intentions prove to be slow-moving and laborious. A crisis does however make changes at chain level possible, but we usually let that opportunity slip through our fingers because crisis management demands our attention.

Put simply, chains form a bleak working environment. But that is nonetheless where the computerisation of society is to a significant extent taking place, with all the accompanying consequences for the quality of life in the future information society.

Topical chain issue: a central European criminal registry?

In July 2004 we were all shocked to learn of the case of Fourniret, the French serial killer who, after serving several long prison convictions, moved to Belgium and continued his murderous activities as the caretaker at a primary school. Apparently, his French criminal record had not been checked before he was given the job. Amidst the general outcry, a number of EU member states called for a central European criminal registry. The idea is that everybody would then know what's what. This is a common response to a social problem: set up a central register for each problem and that's that. In the mid-nineties in the Netherlands, for example, the Dutch Liberal party called for a central national database for sex crimes. At that time, too, the idea was warmly supported, both by the then Minister of Justice and by the civil service[5]. The downside of a central information system of that nature is that it is not possible to register and keep all relevant substantive information up-to-date on such a huge scale. Moreover, we often have too little time to check all sorts of databases in order to ascertain whether there is something we have to take into account in a concrete case. That is why central databases prove to be of little use in practice.

Why should we expect anything of a central criminal registry for the European Union if each EU country already has its own central registry of its own criminal convictions? The registration of convictions cannot therefore be the problem. Apparently, the problem is the exchange of that information across national borders. And perhaps even more: the cross-border use of information about criminal convictions when making concrete decisions, such as when appointing a Frenchman as a caretaker at a Belgian school, or the Belgian judiciary's decision to rule out a Frenchman as a suspect for a Belgian crime.

Exchange of information

So change is needed, but how? On 19 July 2004, the heading of NRC[6], a Dutch national newspaper, read: "Donner prefers the exchange of national information to a new European criminal registry". Indeed, why further centralise the storage of information about criminal convictions within the EU when what is most needed is better communication? In December 2004 the Ministers of Justice and Home Affairs of the European Union decided that information about all criminal convictions in the European Union would henceforth be referred directly to the Ministry of Justice of the convict's country of nationality within the EU[7]. A choice was made, then, to concentrate the criminal record of an EU citizen at the Ministry of Justice of the country of nationality rather than to institute a central European criminal registry. Other EU countries can call up information about a person's criminal convictions in any of the twenty-five Member States in the convict's country of nationality. According to this agreement, that information must be

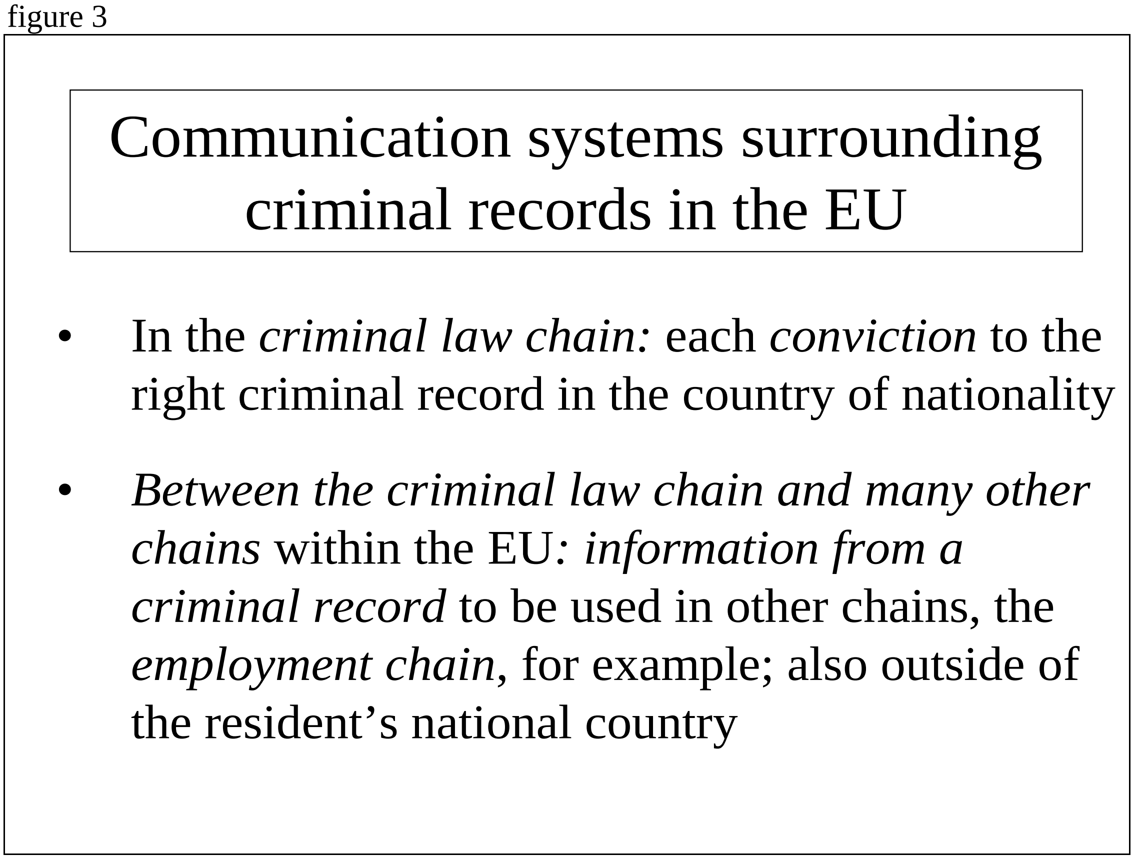
issued immediately, but within ten working days at the latest. Furthermore, a central authority may request information from the criminal records of another Member State.
Does this solve the communication problem concerning convictions details? What stands out here is that the agreement in its current form leads to a better-organised way of registering criminal records. Why, then, should this agreement lead to better prospects for the cross-border use of information on criminal convictions when making concrete decisions outside the domain of criminal law? After all, in the Fourniret case, that is precisely where it went wrong, upon his appointment as a school caretaker.

Chain communication

As the nationality principle has been chosen as the basis of the registry of criminal records in the EU[8], there are two hurdles to be taken for the chain communication involved (see figure 3):

1. a new *criminal conviction* in one of the twenty-five Member States must lead to an addition being made to the right criminal record at the Ministry of Justice of the country of nationality: this transfer of information about a conviction takes place within a single chain, the criminal law chain, but throughout the EU;
2. it must subsequently be possible for someone's criminal record to be used in all EU countries when decisions such as appointing someone as a school caretaker are made. For this communication the criminal law chain is to exchange information with a second chain, depending on the decision to be taken, in this example the *employment chain*.

figure 3



Communication systems surrounding criminal records in the EU

- In the *criminal law chain:* each *conviction* to the right criminal record in the country of nationality
- *Between the criminal law chain and many other chains* within the EU*: information from a criminal record* to be used in other chains, the *employment chain,* for example; also outside of the resident's national country

We thus see that the improved exchange of information concerning the national criminal records of the European Union calls for two different chain communication systems at EU scale. We have not yet gained much experience of chain-computerisation systems of that nature. At least, there are no examples of success at this level that I am aware of. Nevertheless, according to the insights of *Chain-computerisation in the constitutional state*, selective communication systems concerning criminal records to prevent many flawed decisions in chains outside the domain of criminal law do indeed have a good chance of success. This cannot be said for a centralised European criminal registry.

Identity fraud as a major chain problem

Let us take a closer look at hurdle 1, each conviction to the right criminal record at the Ministry of Justice of the country of nationality. This concerns identity fraud as a dominant chain problem in the law enforcement chain. Identity fraud means that somebody with dishonest intentions deliberately passes himself off under an identity that does not belong to him by using the identity of another existing or fictitious person. The identity fraudster can make use of other people's identity documents, personal numbers, and photos, actions or occurrences can be used as well, because they all feature an identity suggestion from which people draw conclusions about whom they are dealing with. Therefore, identity fraud can take place anywhere and in many ways and is not restricted to specific situations, procedures or documents. Once a person has fraudulently changed his identity, the new 'identity' can affect other situations along regular channels. In these situations it usually is no longer possible to see through the preceding fraudulent identity change. The real problem is that if an identity fraud succeeds, all clues and traces lead to the victim who subsequently has much difficulty in proving his innocence. At the moment we lack institutions, methods, professionals and powers that enable to quickly investigate a case of identity fraud and to accurately distinguish between honest victims and pretending culprits and to initiate appropriate action. Thus, identity fraud forms a major threat to our information society[9]. If criminals succeed in using other identities than their own in the criminal law enforcement chain, criminal records are incorrect, incomplete or downright misleading, and the agreed EU criminal registry will not prevent criminals continuing their crimes undetected after moving to another EU Member State. This problem is further aggravated if chances of successful identity fraud by criminals are better when caught committing crimes abroad.

Chain analysis of conviction communication in the EU

The first communication hurdle (each conviction to the right criminal record at the Ministry of Justice of the country of nationality) can, indeed, only be taken cleanly if a foreign criminal conviction is 'booked' for the right person. This is where biometrics comes in, the identification or recognition of individuals based on a physical characteristic using information technology to quickly digitise this physical characteristic so that we can either depict it as an image or subject it to calculations[10]. Getting an EU-conviction faultlessly booked for the right person is only possible if a thorough biometric verification[11] is performed with forensic precision *from* or *in* the country of the suspect's nationality at the beginning of every criminal case anywhere in the EU. Even in someone's own country that often turns out to go wrong. In the Dutch case, the forensic fingerprint verification system HAVANK (named after the famous Dutch author of crime stories) provides for each set of fingerprints a list of all aliases that a person has used in Dutch criminal cases. HAVANK contains thousands of sets of fingerprints that are related to more than one set of person identifying details (family name, first name, date of birth, place of birth, etc). Record-holders in the use of aliases in the Dutch HAVANK system are criminals with 54 aliases. This has not been considered a serious obstacle to legally proving that a suspect is the culprit. But as soon as one wants to accurately communicate about someone's criminal convictions, aliases can only cause mistakes. In the criminal record registry criminal convictions are thus spread across as many separate criminal records as the number of aliases used. These records cannot be straightforwardly merged or combined to get the complete picture without making serious mistakes. This is because we, unfortunately, cannot establish from the administrative records which of those aliases is someone's true identity. And neither can the administrative records tell us unequivocally whether an alias corresponds with a real identity of an accomplice or an innocent victim, or whether it corresponds with a fictitious identity that has found its way somehow into the judicial documentation. To complicate this further, many sets of person identifying details are related to more than one set of fingerprints! This means that an identity has been used by two or more criminals. This puzzling problem of identity fraud in the criminal law enforcement chain is rooted in the chain condition that criminals do not heartily cooperate with law enforcement authorities. Therefore, this problem of identity fraud by criminals probably exists in every EU-country, although the extent of it may vary. Some countries might not even be aware of the problem, at least at political or administrative levels.

figure 4

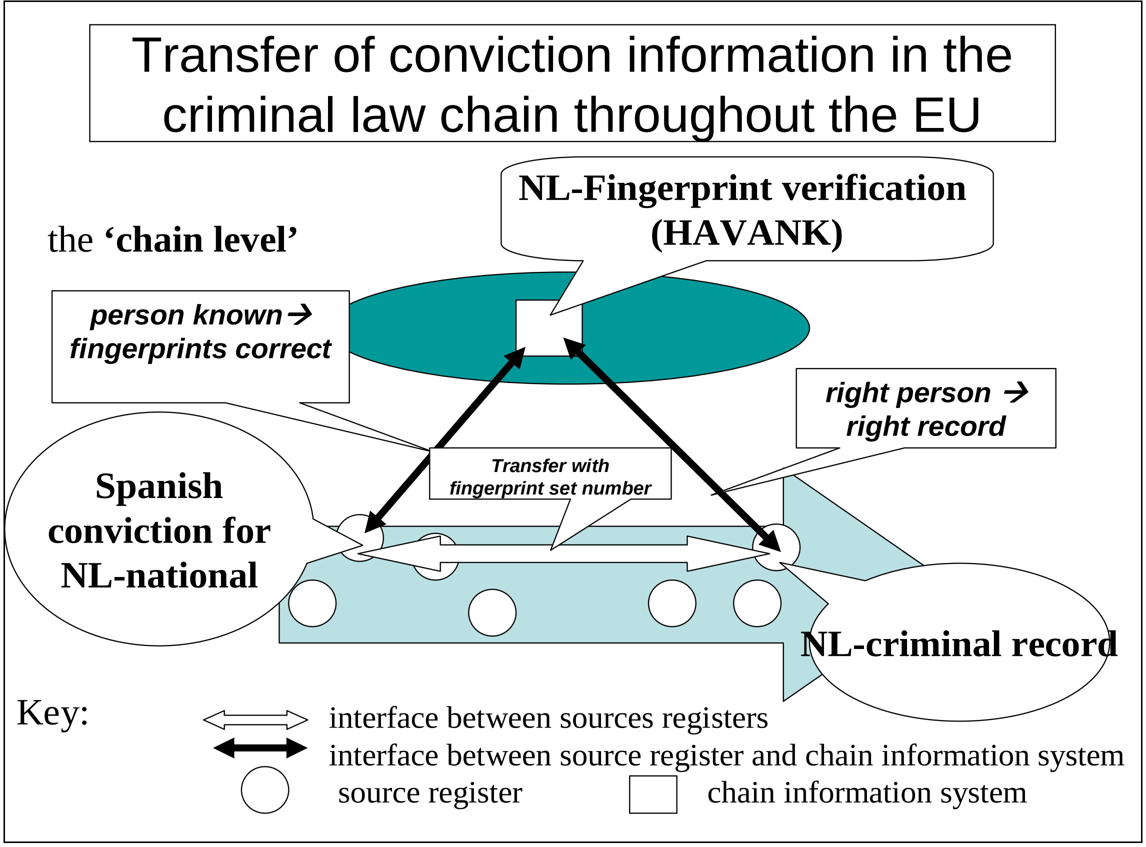

Transfer of conviction information in the criminal law chain throughout the EU
NL-Fingerprint verification (HAVANK)
the 'chain level'
person known → fingerprints correct
right person → right record
Transfer with fingerprint set number
Spanish conviction for NL-national
NL-criminal record
Key:
interface between sources registers
interface between source register and chain information system
source register
chain information system

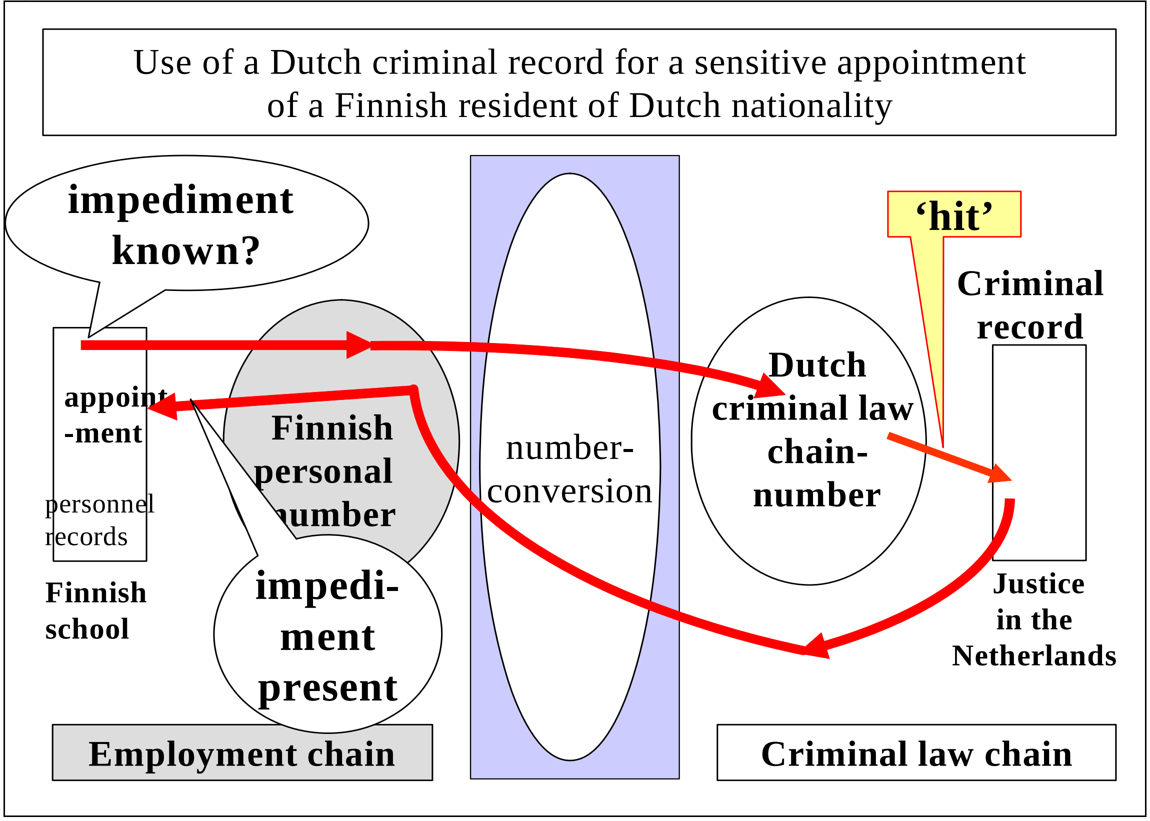
Figure 4 shows how a Spanish conviction concerning a Dutch national ends up in the right criminal record within the Dutch criminal registry. At chain level, only forensic fingerprint verification in the Netherlands can guarantee that the Spanish conviction details are added to the criminal record of the right person in the Dutch criminal registry by making use of the HAVANK fingerprint number that uniquely identifies the criminal's fingerprint set and provides a complete list of his already known aliases. An EU-wide information infrastructure featuring remote forensic fingerprint verification from or in the country of nationality thus proves to be an absolute necessity. This enables the addition of the correct unique national fingerprint number to the case details and to focus the attention of foreign authorities on the need of a thorough identity investigation to make sure that the new conviction will eventually be added to the right criminal record. Otherwise, the more cunning criminals will increasingly commit crimes outside their national country and when caught, will seize the opportunity to use alias identities which cannot easily be refuted outside the national country, in order to keep their own criminal record clean or as short as possible.

Thus, at EU scale this communication system underlying the addition of any new conviction to the right criminal record in the right national criminal register is in itself an unprecedented challenge. But that is not yet enough to solve our communication problem.

Chain analysis of the use of criminal records in the EU

Hurdle 2, making the right decision taking into account relevant information from the right criminal record, calls for communication between the European criminal law chain and an *alternating* second chain in one of the EU-countries, depending on the decision

figure 5



to be taken. That is because the criminal record, now rightly located in the correct national criminal register somewhere in the EU criminal law chain, has to be actually used for decisions in *all sorts of other chains* in any EU country, such as in the Finnish 'employment chain', for the appointment of a Dutchman as school caretaker in a Finnish city. This example is shown in figure 5.
We further assume that Finland uses a Finnish personal number to uniquely identify every resident regardless of his nationality. Number systems are needed for information processing and communication relating to natural persons. They are getting more widely used as means of person recognition, off line and on line. By using a number it is possible to trace a detail or establish that two details belong to each other, for verification purposes for example. Verification is much more effective with numbers than only with words (name and address details) or images (photograph, signature, logo). Comparing numbers can prevent or reveal errors when linking details about the same persons, objects or occurrences. The number can also prevent confusion from arising when it is difficult or impossible to write down an identifying personal detail in a straightforward manner. Examples include when information systems use a limited number of letter characters or when foreign sounds can be rendered in various ways. Number systems also provide means to keep some personal details separate from other details for reasons of security or privacy. These many important functions of number systems causes number systems theory to be an important part of the body of knowledge embodied in *Chain-computerisation in the constitutional state*[12].

We further assume that every EU country uses a criminal law chain number, like we actually do in the Netherlands, to uniquely identify every criminal in the country's criminal law enforcement chain. A Finish resident of Dutch nationality will have to have his criminal record screened in the Dutch criminal register for risks related to his appointment in Finland. In Finland his Finnish personal number serves as point of departure for this procedure. Using his Dutch identifying personal details, an automatic verification in the Netherlands is done of whether he has been assigned a Dutch criminal law chain number. This is only the case if he has a Dutch criminal record and the criminal number then provides the administrative link to this record. It is only if there is an appointment relevant 'hit' in his Dutch criminal record that the Finnish decision-maker is notified *that* there are impediments, but not *what they are*. In this communication system, number conversion from the Finnish residents' number into the Dutch criminal law enforcement number, and vice versa, makes it possible to keep the information infrastructure of the employment chain separate from that of the criminal law chain, in Finland as well as in the Netherlands.

Chain-computerisation as approach

This example clarifies the complexity of our society when viewed from the perspective of large-scale information exchange. Although the concept 'chain' is of course no more than a mental construct, it can be used to show the way in the complex chain landscape of our emerging information society. Unfortunately, a more simplistic approach does not alter this complex reality. The example of the EU criminal registry can stand as a model for other vital communication complexes, for instance those related to identity records and patient records. These huge communication systems form cornerstones of our future information society. The discipline *Chain-computerisation in the constitutional state* provides tools that can be used to design and create these communication systems. If this field of study can help with the development of these three social priorities (criminal record, identity record and patient record) in the years to come, the chair of *Chain-computerisation in the constitutional state* at Utrecht University will have fulfilled its mission.

There are still too many people who believe it is necessary to stuff all of the information in a chain into a single database. At this enormous scale, that yields little more than a concentration of management activities, not communication. And that management must be carried out by people who have barely any affinity with the registered details. It would be much better if all parties in a chain collected and managed their own information. A single, collective registry will not work at this scale. Information must stay with the owner and be managed there too. At the same time, chains need a central access system, including a method for signals and alerts, so that other parties in the chain can gain access to the essential information when necessary. What is remarkable here is that the access mechanism differs between chains. For someone who has had a heart attack, it is important that a small number of details are immediately available to the treating doctor so that he can effectively intervene. The chain will therefore have to be able to supply those details as quickly as possible. That communication system is completely different from that for diabetics, for instance. For the correct treatment of a wide range of ailments for the rest of a diabetic's life, many different care providers require highly varied details.

Chain-computerisation is different from traditional approaches

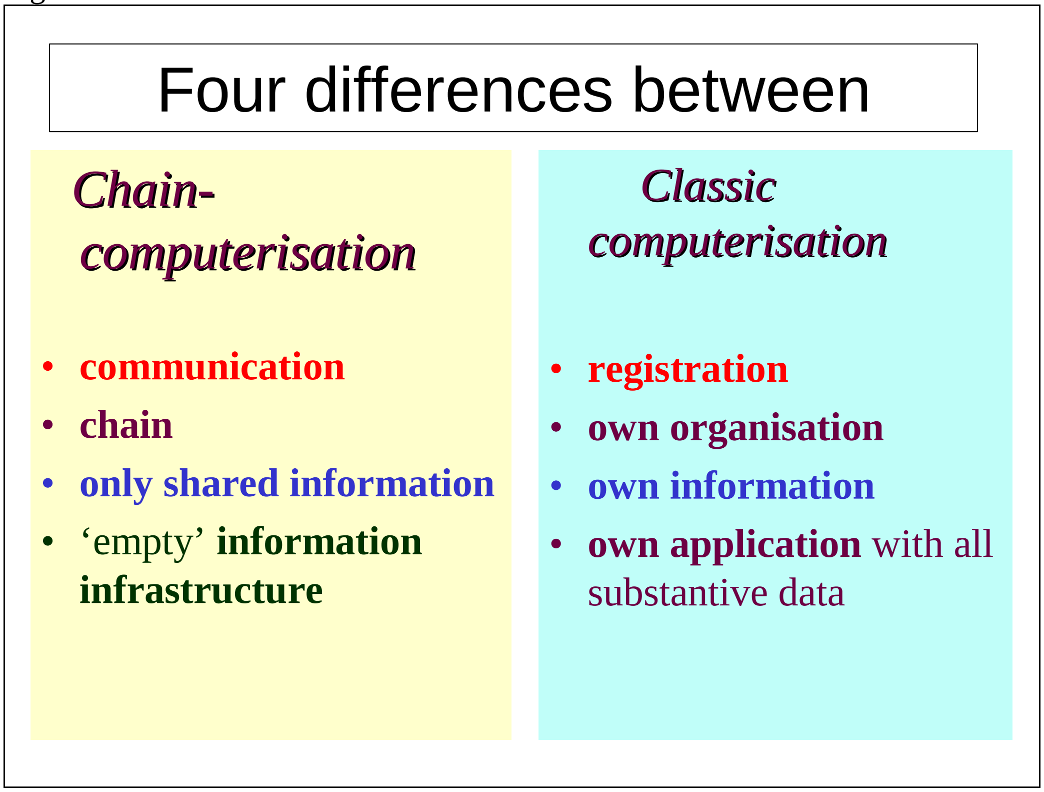
Chain-computerisation, then, relates above all to structuring and automating the communication needed for the mutual exchange of the information required by all participants in the chain. In that respect, chain-computerisation is essentially different from the usual approach of computerisation. Figure 6 shows the four most important differences.

First of all, chain-computerisation focuses on the *communication* of just a few details that are critical to the chain, rather than on the *registration* of these and other details. The key question here is where the necessary piece of information can be obtained at the right moment from elsewhere in the chain in order to avoid a wrong decision at the right place. The question of how that piece of information must be registered and managed somewhere in the chain does not play any particular role in that respect.

Secondly, in chain-computerisation everything revolves around the *chain*, rather than the *individual organisation*. The analysis of information problems and the development of information systems are traditionally based on the client's internal organisation. Conversely, chain-computerisation opts for the external collective 'chain level' as the starting point and focuses on the dominant chain problem. 'Chain-computerisation' assumes that each chain partner takes his own computerisation process seriously and does not therefore compete with the customary, organisation-oriented approach of automation by the chain partners. 'Chain-computerisation' supplements it with a chain-specific communication system that brings about communication between the parties when necessary, rather like a traffic regulator.

The third point of difference concerns the data. 'Chain-computerisation' focuses exclusively on the essential *collective data*, and even then only to the extent that they are indispensable to tackling the relevant dominant chain problem. Conversely, organisations are primarily accustomed to bringing together and managing *all of the substantive data* that they need in their work.

figure 6



Four differences between

Chain-computerisation

- **communication**
- **chain**
- **only shared information**
- ‘empty’ **information infrastructure**

Classic computerisation

- **registration**
- **own organisation**
- **own information**
- **own application** with all substantive data

Finally, the fourth point of difference. A critical piece of information can only be made directly available at the moment of a decision or action by means of a chain-specific, ‘empty’ *information infrastructure* that is geared to the dominant chain problem to be collectively tackled. ‘Empty’ means that only essential data without much content are present at the chain level. With a reliable patient number at chain level, for instance, it is possible to establish whether each new prescription shows any contra-indications in the light of all current prescriptions for that patient, even though the details of his medicines are held in dozens of different *internal information systems* owned by pharmacists and physicians.

Chain-computerisation ‘in the constitutional state’

In addition to these four points of difference between chain-computerisation and traditional approaches to the computerisation of large-scale information exchange, chain-computerisation requires fundamental legal principles to serve as the starting point or, in other words, as design criterion for information infrastructures for large-scale chain communication. This can be clarified by way of example. Megan’s law was signed by President Clinton on May 17 1996 for the protection of children[13]. The law was named after a seven-year-old girl who was raped and murdered in 1994. The perpetrator – with two previous convictions for paedophilia – lived in the house opposite the victim’s. Megan’s Law requires the States to register individuals convicted of sex crimes against children and allows the States discretion to establish criteria for disclosure, but compels them to make private and personal information on registered sex offenders available to the public. This American law apparently interprets the idea of ‘communication’ as ‘broadcast’. In our legal culture, we generally take the view that this form of exchanging sensitive personal information is not legitimate. Chain-computerisation in the constitutional state views communication as ‘signalling’ or ‘alerting’ somebody if he has to make a concrete decision that could turn out badly without that critical information. The metaphor of private ‘mail’ is more appropriate than that of public ‘broadcast’ to this signalling process. A neighbour with children does indeed need to be alerted, but the dissemination principle of public broadcast of Megan’s Law is rarely the right - and certainly not the only - response to a pressing social need for better communication.

In the practical case of the EU criminal record we saw that in the communication from the one chain to the other, the one chain number was converted into the personal number of the other chain. Personal details from the criminal law chain, for instance, are thus hidden from authorities in the employment chain. The number conversion ensures that personal details from the one chain cannot simply be linked to details from another chain. Chain-computerisation in the constitutional state, then, opts for the protection of people’s private lives as a starting point for communication solutions by applying at chain level the principle that data may only be used for the purpose for which it was collected. In figure 5 number conversion prevents the presence of a criminal law chain number or a criminal record from being visible in the employment chain, while making it possible to issue an alert if necessary. Whether this chain communication solution will actually work does of course depend on all sorts of other factors, too, such as the chance of identity fraud being committed in the process of migration within the EU. After all, a citizen with a criminal record is not necessarily going to be a heartily cooperative citizen. He may try to rid himself of his criminal record. If we do not succeed in establishing a communication system around criminal convictions that is up to preventing identity fraud, serious crime will shift to the neighbouring country offering the best chance of keeping one’s criminal record clean. With the EU criminal record based on the country of nationality principle we then jump from the frying pan into the fire.

International chain offshoots and interpenetrations: reciprocity

‘*In the constitutional state*’ also has a second meaning. Social chains are gaining more and more international offshoots and interpenetrations. If the law serves as the starting point for chain information infrastructures, it will become increasingly often the case that several legal cultures, which are sometimes difficult to reconcile, are found within the same chain or in the same communication system. This is something that must be taken into account with chain-computerisation. In practice, we are confronted by this in the demands of the US regarding travellers’ details. What is required here is greater understanding of the ways in which various legal-cultural starting points can be given a place alongside each other in computerised chain communication. As things stand, we often choose the solution of the party that has the greatest say in the matter. But insofar as these legal-cultural differences relate to EU countries mutually, that is not a future-proof strategy. After all, within the EU we generally base our approach on the principle of reciprocity respecting each other’s values and norms.

Some conclusions

An EU communication system around criminal convictions based on the country of nationality that is up to preventing identity fraud, is a major challenge. With similar systems around identity records and critical medical records, this communication system is an important cornerstone of our future information society. Unfortunately, we know precious little about information exchange on this enormous scale requiring better concepts, theories and strategies that can explain why so many large-scale projects and systems fail. *Chain-computerisation in the constitutional state* can provide some of these tools and insights by taking closer account of the specific problems of large-scale information exchange and cross-border cooperation in chains.

The chain-analysis of the necessary information exchange around criminal convictions based on the country of nationality presented here, demonstrates that unless we adopt additional precautions the volume of identity fraud in criminal cases involving nationals abroad will substantially increase. This will cause national criminal records to be more often incomplete and incorrect, resulting in wrong decisions, for instance in relation with sensitive appointments like Fourniret's. Then the agreed EU communication between national criminal registries will not prevent criminals from continuing their crimes undetected by committing cross-border crime or by moving to another EU Member State.

An EU-wide information infrastructure featuring remote forensic fingerprint verification *from* or *in* the country of nationality proves to be an absolute necessity to enable addition of the correct unique national fingerprint number to the case details and alerting foreign authorities to the need of a thorough identity investigation to make sure that the new conviction will eventually be added to the right criminal record. Otherwise, the more cunning criminals will increasingly commit crimes outside their national country and when caught, will seize the opportunity to use alias identities which cannot easily be refuted outside the national country, in order to keep their own criminal record clean or as short as possible. After all, a citizen with a criminal record is not necessarily going to be a heartily cooperative citizen. He may try to rid himself of his criminal record. If we do not succeed in establishing a communication system around criminal convictions that is up to preventing identity fraud, serious crime will shift to the neighbouring country offering the best chance of keeping the criminal's record short or clean.

The insights derived from this chain-analysis thus prove to be essential for an effective and consistent European system of cross-border use of national criminal registers.

[1] This article appeared in in: European Journal of Crime, Criminal Law and Criminal Justice, Volume 14 (2006) 1, Brill Academic Publishers, Leiden ISSN 0928-9569. It is based on my inaugural address delivered on the occasion of the public acceptance of the endowed chair of *Chain-computerisation in the constitutional state* at Utrecht University, J.H.A.M. Grijpink, *Our emerging information society*, the challenge of large-scale information exchange in the constitutional state, Utrecht, January 2005, ISBN 90-393-0049-6; the main body of the text of the inaugural address has been published in: Computer Law and Security Report, vol. 21 (4) 2005, Elsevier Science Ltd, Oxford, UK, ISSN 0267-3649

[2] Prof. dr. *mr* J.H.A.M. Grijpink (1946) studied Economics (1969) and Law (1971) at Groningen University. He obtained his Ph.D. in 1997 at the Technical University Eindhoven for his thesis Chain-computerisation. He is Principal Advisor at the Strategy Development Department of the Dutch Ministry of Justice and Professor of information science at Utrecht University. He is a Certified Management Consultant (CMC) and Registered Information Expert (RI).

[3] J.H.A.M. Grijpink, *Keteninformatisering* ('Chain-computerisation'), Sdu, The Hague 1997;
J.H.A.M. Grijpink, *Werken met keteninformatisering* ('Working with Chain-computerisation'), Sdu, The Hague 1999, and
J.H.A.M. Grijpink, *Informatiestrategie voor ketensamenwerking* ('Information Strategy for Chain Cooperation'), Sdu, The Hague 2002.
A brief introduction in English is published in two articles in Information Infrastructures & Policy 6 (1997-1999), IOS Press, Amsterdam, March 2000: (1) *Chain-computerisation for interorganisational policy implementation* and: (2) *Chain-computerisation for better privacy protection.*

[4] This follows the approach that Lionel Robbins applied to the positioning of economics as a science in *An essay on the nature & significance of economic science*, MacMillan & Co, London, 1932. The analysis level that the sub-discipline chain-computerisation focuses on is called the 'chain-level'; its basic aspect of study is large-scale automated communication; the specific focus of study is the information-structure and specific concepts are 'chain' and 'dominant chain problem', for instance. The so-called 'chain laws' can be considered as examples of the sub-discipline's own typical theories.

[5] Quote: "VVD member Korthals […] presses for a national database for sex offences at the Central Criminal Information Department (CRI). The CRI itself has been calling for that for longer because the police cling too much to incidental cases", NRC Handelsblad, 22 August 1996, p. 3

[6] NRC Handelsblad, 19 July 2004, p. 1

[7] Counsel of the European Union, Press Release, 2626th Counsel Meeting, Justice an Home Affairs, Brussels, 2 December 2004, 14894/04 (Press 332)

[8] In the original text of my Inaugural Address I presented a chain analysis assuming the country-of-residence-principle as the basis of the EU-criminal registry. This chain analysis becomes more relevant in the long run, as the system will have to take into account the EU-exchange of information about criminal records of EU-residents not (yet) being EU-nationals.

[9] J.H.A.M. Grijpink, *Identity fraud as a challenge to the constitutional state*, in: Computer Law and Security Report, vol. 20 (1) 2004, pp. 29-36, Elsevier Science Ltd, Oxford, UK , ISSN 0267-3649

[10] Checking someone's identity biometrically involves comparing a previously measured physical characteristic with the result of a new measurement at the time and place of the check. Biometrics offers many alternatives for protecting our privacy and preventing us from falling victim to crime. Biometrics can even serve as a solid basis for safe anonymous and semi-anonymous legal transactions. As yet biometrics technology cannot be safely applied at large-scale. The reader is further referred to my articles:
J.H.A.M. Grijpink, *Biometrics and Privacy*, in: Computer Law and Security Report, May/June 2001, vol. 17 (3) 2001, pp. 154-160, Elsevier Science Ltd, Oxford, UK , ISSN 02673649, and
J.H.A.M. Grijpink, *Two barriers to realizing the benefits of biometrics*: A chain perspective on biometrics, and identity fraud as biometrics' real challenge, in Optical Security and Counterfeit Deterrence Techniques V, edited by Rudolf L. van Renesse, Proceedings of SPIE-IS&T Electronic Imaging, SPIE Vol. 5310, pp. 90-102 (2004). Also in: Computer Law and Security Report, vol. 21 (2 and 3) 2005, Elsevier Science Ltd, Oxford, UK, ISSN 0267-3649

[11] The future biometric passport and identity card with two fingerprints on it as the only means of biometrically checking someone's identity is not secure enough to safeguard us from identity fraud. This implies that one cannot trust the administrative identifying personal details from an identity document alone to accurately direct a foreign criminal conviction to the right criminal record in the country of nationality.

[12] J.H.A.M. Grijpink, *Personal numbers and identity fraud, number strategies for security and privacy in an information society,* Part I en II, in: Computer Law and Security Report, vol. 18 (5 en 6) 2002, pp. 327-332 en pp. 387-395, Elsevier Science Ltd, Oxford, UK , ISSN 02673649

[13] NRC Handelsblad, 3 December 1998, Profile, p. 2; more recent information on can be found at http://www.klaaskids.org/pg-legmeg.htm