ISSN 1879-9523
journal of chain-computerisation
information exchange for chain co-operation
Universiteit Utrecht

Scientific article

Chain-computerisation in practice: the criminal justice chain

W.L. Borst

Journal of Chain-computerisation
Information Exchange for Chain Co-operation

2011 – Volume 2, Art. #10

Received: 1 March 2011
Accepted: 1 April 2011
Published: 14 April 2011
Translation: Sandra R. Reijnhart

2011 – Volume 2, Art. #10
URN:NBN:NL:UI:10-1-101415
ISSN: 1879-9523
URL: http://jcc.library.uu.nl/
Publisher: Igitur publishing in co-operation with the Department of Information and Computing Sciences

Chain-computerisation in practice: the criminal justice chain

W.L. Borst
Ministry of Security and Justice
Post-box 20301, 2500 EH Den Haag, the Netherlands
E-mail: w.l.borst@minjus.nl

Abstract: Criminal law enforcement can be seen as both a chain and a network. The 'chain' concept is the guiding principle for the design of the information-architecture and the computerisation of the chain. Originally, the dominant chain problem was the ability to administer the correct sanction (punishment or action) to a person (perpetrator). Since 2005, a new perspective has been added to this: the accurate and reliable identification of suspects and convicted persons, because it is essential to administer the sanction to the right person. The administration of the right sanction requires full and adequate information about the suspect. Much of this information is already available within the organisations that together form the criminal justice system. However, the information must be made available -- quickly and easily -- to those who need it. This information is designated as "the comprehensive (criminal) picture of the person'. Imposing the penalty to the right person also demands a watertight system for establishing the correct identity of suspects and convicted persons throughout the entire chain of criminal justice, preventing the use of aliases to get rid of a sanction or a reputation. This information is designated as a person's 'correct (criminal) picture of the person'. The theory of Chain-computerisation offers us the necessary concepts and insights for the design of the requisite information architecture for achieving both these profiles. This article deals primarily with the latter: the correct (criminal) picture of the person'

Keywords: Criminal justice chain, chain-computerisation, exchange of information, biometrics, profile, identity management, identification

1 Introduction

In this article, "chain" and "network" are seen as complementary– and not competing – concepts. The network concept does not, in itself, provide any guidance for the intrinsic interpretation of the co-operation between involved parties, and even less for the computerisation; the chain concept does do that. The purpose of this contribution is to illustrate this statement on the basis of the Dutch chain of criminal justice.

2 The criminal justice system as chain and network

The criminal justice system is one of the purest examples of a chain. The process is basically very simple:

investigate → *prosecute* → *try* → *execute (the sentence)* → *reintegrate*

Every previous step is an essential – but not necessarily also sufficient – condition for every following step. This can easily be understood. After all, reintegration follows detention; detention can only be executed on the basis of a judicial

decision; but a judge can only arrive at a decision if the case is presented to him by a prosecutor; and a prosecutor cannot bring a criminal case to court if he has not received sufficient material from the investigation.

Thus, the chain as a process is, in itself, simple. What makes the criminal justice chain complicated is the large number of actors. Criminal law is implemented by hundreds of parties that are all autonomous with respect to each other. To complicate matters further, it is also the case that criminal justice jurisdiction, by law, is generally not attributed to organisations but to functionaries. Just take this example: You will not find the term "police" in the Code of Criminal Procedure; the Code consistently refers to 'the investigating officer.' However, that term does not only refer to the police (about 50.000 officers, scattered over 26 police forces), but also to the Royal Military Police (about 6000 officers), the four special investigation services (in all, several hundred officers) and, moreover, another 25.000 special investigating officers ("boa's") who work in more than 1000 organisations. Of all of these organisations and functionaries, there is not one who can complete the chain product 'the criminal justice intervention' on its own. In the past, if you got a ticket on the streets, you could pay the policeman in cash. In this way, the policeman executed the entire chain product by himself (just as I discovered when, as a 15-year old school boy, I cycled to school 'with no hands…'). These days, that is completely impossible.

We must now all rely on co-operation. A network originates because individuals or organizations cluster around shared values and/or interests (Van der Steen et al., 2009:30). It is clear that that is also addressed in the administration of criminal justice. The administration of criminal justice is, therefore, *both* 'chain' and 'network' (Borst, 2010). The network originates at the moment that the parties seek each other out for consultation, co-operation, etc.; as long as they are satisfied to simply pass cases along, there is no question of a network.

3 The dominant chain problem is shifting

In the administration of criminal justice, it is desirable, wherever possible, to deal simultaneously with all the cases that could be pending against a suspect as interrelated instead of as isolated cases. That enables individualized intervention which is considered to benefit the effectiveness – and in many cases also the efficiency – of the administration of criminal justice. This insight, of course, existed long before the Security Programme of the Balkenende Cabinet I (in October 2002) launched the 'personalised approach.'

As early as the beginning of the 1990s -- under the leadership of the man whose retirement is the occasion for this contribution -- the 'chain-wise' computerisation of the criminal justice chain was initiated. A Criminal Justice Reference Index of Persons [VerwijsIndex Personen strafrecht handhaving, VIP] was created that consisted of two components: A collection of (sets of) personal details of suspects ("identifying personal details": name, address, date of birth, etc.) and a collection of references. The steppingstone is the VIP number. After all, "*without number systems, identity management is unthinkable*" (Grijpink, 1999, p. 155). The identifying personal data are, where possible, checked with the authentic registers: The Municipal Personal Records Database (GBA) or the Basic Provisions for Aliens (BVV). The references indicate which chain parties are currently dealing with a case against a specific suspect or convicted person.

In the past decade, a dimension has been added to this. There were sundry signals pertaining to a number of problems with respect to the identity of suspects and

convicted persons. A number of them have, of course, been known for a long time, such as the fact that in HAVANK, the automated fingerprint system of the Dutch Police, sets of fingerprints appear that sometimes have dozens of names registered to them. Midway through the first decade of this century, the problem of identity fraud in the criminal justice chain escalated. And thus, the theme of identification rose to the surface as a dominant chain problem.

Chain-computerisation is a theoretical framework that is ideally suited to tackle this. After all, the general 'chain law' is: "*Problems and errors have a tendency to travel downstream*" (Kumar & Van Dissel, 1996, p. 284). If that is the case, that also provides leads for tackling this problem, namely:

- Nail up the chain down in the front;
- Follow the suspect though the entire chain.

Here, too, is the steppingstone: the criminal client number, denoted in the legal system as the criminal chain number (SKN; this is the successor to the previously mentioned VIP-number).

4 Architecture of chain-computerisation: three levels

The creation of a criminal justice reference index led to a chain architecture at two levels (Grijpink, 1999):

- The 'base level of the chain' of the individual parties and their information systems and
- The 'chain level'; that is the reference index with connections to registers outside the chain.

The reference index only represents the current situation. Moreover, there is a historic archive in the criminal justice chain that contains the previous decisions of public prosecutors and judges in criminal cases: the Criminal Records System (JDS). If you consider the reference index to be a sort of satellite that hangs above the chain, then you could think of the criminal records system as the great depository in the cellar of the house. Thus, a third level is added to the chain architecture. This is represented in the diagram below (see Figure 1).

The wide horizontal arrow in the centre represents the primary process; the white dots in it are the information systems of the individual organisations. The Criminal Records System is the 'archive' of the chain. The chain registration of personal data contains the identifying personal data, the reference register contains the current references (current cases, currents events). Together, these two registers form the Criminal Justice Chain Data Base (SKDB; previously VIP: Criminal Justice Reference Index of Persons). The solid arrows indicate the data exchange; the dotted arrow is the connection between the SKDB (current situation) and the Criminal Records System, pertaining to the identity of the registered persons. For, the person about whom the public prosecutor or the judge makes a decision – whether that is a dismissal or an acquittal or a conviction – must, of course, be the same person who initially has been registered as the suspect (for a more extensive explanation, see Borst, 2010, pp. 232-238).

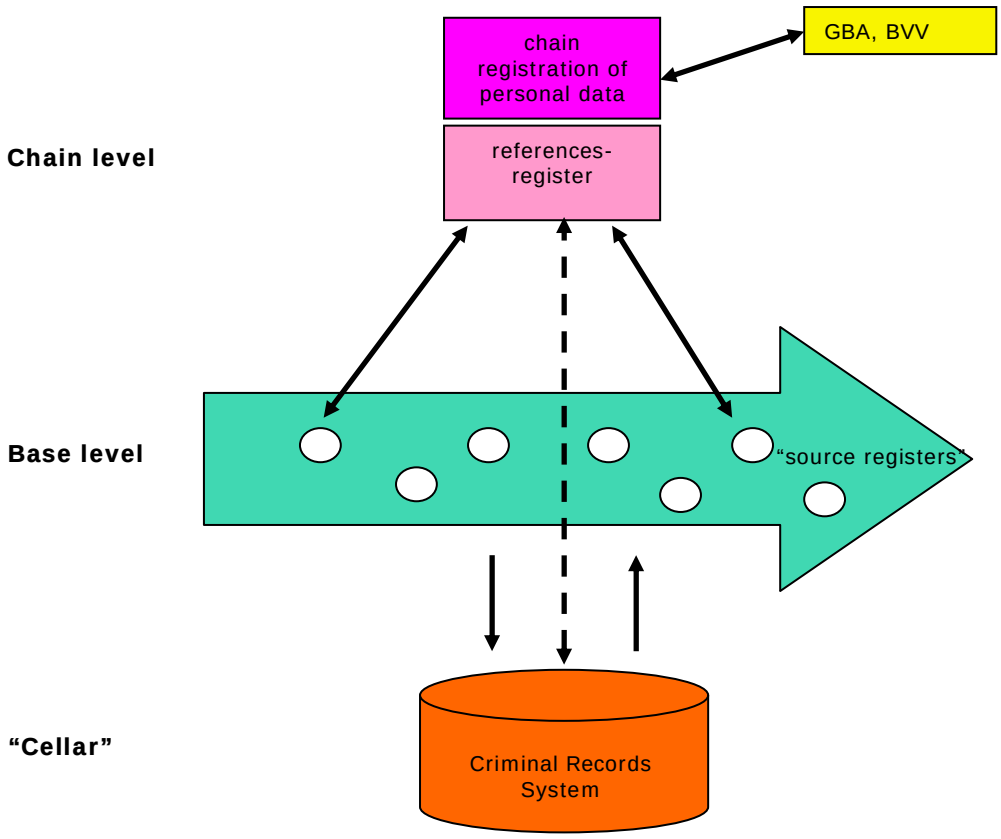

Figure 1: The information architecture of the chain of criminal justice

5 Application to the assessment of the identity

If we then examine the manner in which someone's identity is assessed, then the Act on the assessment of the identity of suspects, convicted persons and witnesses (WIVVG) immediately comes into the picture. This Act – prepared by Minister Donner (who was also in part responsible for establishing the special chair "Chain-computerisation in the Constitutional State), subsequently submitted and defended in Parliament by his successor, Minister Hirsch Ballin, and, on 1 October 2010, put into effect – introduces the following system (Van Deudekom & Borst, 2010):

- Based on the Compulsory Identification Act, everyone aged 14 and older is required, when first asked by an investigating officer, to offer identification for inspection. This requirement also applies to suspects. If a suspect is detained and brought to the police station for questioning due to suspicion of a crime for which pre-trail detention is permitted (these are all crimes that could be punished with a prison sentence of four years or more) then, in order to establish his identity, his identity papers are requested and he is also photographed and fingerprinted. If someone is fingerprinted for the first time, the fingerprints are then linked to a new criminal justice chain number (SKN).
- The SKN is, in those cases, issued on the basis of biometric identification. Herein lies an essential difference with the general identity chain, where fingerprinting is only done long after the person in question has been assigned his citizen service number (het BSN), namely, at the moment that

the person in question applies for identity papers. The BSN itself is granted without any connection whatsoever to biometrics, namely at the moment that the birth of a child is registered (based on assertion without proof).

- If there is no question of a crime for which pre-trail detention is permitted, the request for access to identity papers is then sufficient (without photographing or fingerprinting), unless there are doubts about the identity of the suspect (then photographing and fingerprinting are done).
- Once a suspect or convicted person has been fingerprinted in order to establish his identity, then his identity will be verified with fingerprint checking at other moments during the legal proceedings. If there are no fingerprints, then identity papers are sufficient as proof of identity.

The identifying personal data are administered for the entire chain by the Judicial Information Service, Department of Matching. This, however, does not apply to the fingerprints; they are administered by the National Police Service Agency (KLPD). The links back and forth are made via the separate numbers: the SKN is recorded in the fingerprints databank; the number of the fingerprints is recorded in the criminal justice chain database (SKDB). This also applies to the DNA profiles of suspects and convicted persons; these numbers are also interlinked (the DNA profiles are administered by the Dutch Forensic Institute). It is determined by law that, if body material is removed from a suspect or convicted person for determining the DNA profile, the identity of the person in question must *always* be verified with fingerprints. In this way, an unbreakable connection is established between the various biometric (physical) personal data. For nothing could be worse for the chain than if a person were registered under ten aliases in the fingerprinting databank and under an eleventh alias in the DNA databank.

The Judicial Information Service receives the identifying personal data and assesses whether or not the person in question is already present in the criminal justice chain database (= matching). This organisation also (on behalf of the minister) allocates the SKN's to the suspect and administers the criminal justice chain database. As the cornerstone of the system, it is stipulated that all parties in the criminal justice chain are bound to use the SKN as the vehicle in the (digital) exchange of information on suspects or convicted person.

6 Conclusion

It should be noted that fingerprints, in this scheme are given a completely new (additional) function. Traditionally, fingerprints have been used as means for investigation and evidence. Fingerprints that are found at the scene of the crime ("clues") were – and are – compared with the fingerprints previously recorded in the files of known suspects. And conversely: fingerprints of known suspects are compared with the available clues in the files. In this way, many crimes can be solved. In the new system, a new function has been added. Under the WIVVG, fingerprints are a recognition tool, not only for investigation and conviction, but for the entire chain. In those cases where a suspect has been fingerprinted at the beginning of the criminal justice trajectory for identification, they will be used -- in a one-to-one coupling to the SKN -- throughout the entire chain in order to verify that the right person appears in all subsequent stages of the criminal justice procedure of his/her case. For instance, when checking in to serve a prison sentence. Thus, practically speaking, it can be guaranteed with maximum certainty that the criminal justice processing and interventions deal with the right person and not with somebody else.

In this way, therefore, the chain is 'nailed up down at the front' as far as the assessment of the identity is concerned and the person is question is followed throughout the entire chain on the basis of his SKN and, if available, his fingerprints -- from the investigation up through the execution of the sentence. Avoiding your punishment by falsifying your identity – or having someone else serve time for you – is, in this way, no longer possible, at least in The Netherlands. For however well organised this system is in The Netherlands, most other countries are still a long way from achieving this. And also, international exchange of data on suspects and convicted persons is still, for the most part, generally being done on the basis of administrative data. Fingerprinting is used only very sporadically in international legal assistance; and not, at this time, in the exchange of, for example, criminal sentences.

Thus, there is still a great deal of work to be done, as Jan Grijpink, (2005; 2006) has repeatedly argued. But be that as it may, just as the criminal justice system is one of the purest forms of a chain, the WIVVG is, no doubt, one of the purest applications of the theory of Chain-computerisation!

Biography: Wim Borst (1953) studied Law (1976) at Erasmus University Rotterdam. He got his PhD at Leiden University (1985) with a dissertation on "The means of evidence in criminal cases." In 2006 he obtained the degree of Executive Master in Information Management (EMIM) at Amsterdam University. He taught criminal law at Leiden University and served as a court legal assistant at the Supreme Court of the Netherlands. At the moment, he is senior policy advisor for the Ministry of Security and Justice.

References

Borst, W.L. (2010). *Jegens en Wegens. Over persoonsgebonden informatie in de strafrechtketen* (tweede druk) [*Towards and because of: On personal information in the chain of criminal justice* (second edition)]. Nijmegen: Wolf Legal Publishers.

Grijpink, J.H.A.M. (1999). *Werken met Keteninformatisering. Informatiestrategie voor de informatiesamenleving* [*Chain-computerisation in practice. An information strategy for an information society*]. The Hague: Sdu Uitgevers.

Grijpink, J.H.A.M. (2005). Our emerging information society: The challenge of large-scale information exchange in the constitutional state. *Computer Law and Security Report, 21*(4), 328-337.

Grijpink, J.H.A.M. (2006). Criminal Records in the European Union, the challenge of large-scale information exchange. *European Journal of Crime, Criminal Law and Criminal Justice, 14*(1), 1-19.

Kumar, K. & Van Dissel, H.G. (1996). Sustainable Collaboration: Managing Conflict and Cooperation in Interorganizational Systems. *MIS Quarterly, 20*(3), 279-300.

Van Deudekom, K. & Borst, W.L. (2010). Wie is het? Wat weten we al van hem? [Who is it? What do we already know about him?] *Ars Aequi 2010 (september)*, 628-634.

Van der Steen, M., Peeters, R. & Van Twist, M. (2009). *De Boom en het Rizoom. Overheidssturing in een Netwerksamenleving*. Den Haag: Ministerie van VROM.