Law and Judicial Records in Israel: Invalid Management and Sharing of Public Knowledge

Joseph Zernik

Human Rights Alert NGO, Tel Aviv, Israel[1]

joseph.zernik@hra-ngo.org

Abstract: Valid management and sharing of public knowledge is a critical aspect for any competent legal system and for the safeguard of human rights. The duty of government to make the law known is commonly accepted legal norm, relative to laws that are enacted by the legislature. Yet, how are laws, which are embedded in cyber platforms by programmers, to be managed and shared? The problem was presented by L. Lessig as a legal theory - "Code is Law". Lessig primarily addressed commercial platforms that were used for sharing knowledge, claiming that such platforms effectively established new rules, which were not enacted through any democratic process, were not explicitly stated, and might threaten constitutional principles. E-government systems are a critical subset of such cyber platforms. Instant case study presents data from a series of Israeli court cases, pertaining to rules that are embedded in e-government systems, which determine tax liability, using the Tax Authority system, and valid signing and entry of criminal judgments of the courts themselves, using Administration of Courts Net-HaMishpat system. In both cases, government agencies refused to provide any information regarding such rules, pursuant to the *Freedom of Information Act*. Following lengthy court battles, such rules have not yet been provided. The Israeli Supreme Court has avoided ruling on the issue whether software or IT system code constitutes "information" pursuant to the *Freedom of Information Act*, deeming it 'not ripe for review and decision'. The obvious concern is that the rules, which are implemented in the respective e-government systems are out of compliance with the publicly shared law and violate constitutional rights. In both cases, the issue is directly related to authentication and validation of e-government systems and the knowledge they share. Such circumstances raise further concerns regarding knowledge management and sharing - lack of integrity and dissemination of invalid public knowledge by governments, undermining the public's capacity to keep a watchful eye on the working of government agencies. Particularly regarding the courts, such circumstances can undermine the rule of law and human rights. IT experts should assume a more active role in human rights protection.

Keywords: Knowledge management, e-Government, Code is Law, Due process, Liberty, Rule of Law, Israeli courts

1. Introduction

Sharing knowledge is a critical aspect of knowledge management. Sharing knowledge is of crucial importance in any competent legal system: First – regarding the duty of government to make the law known (Murphy, 1982); second - regarding the right to inspect and to copy judicial records, which was ruled a constitutional right by the US Supreme Court in *Nixon v Warner Communications, Inc.*, 435 U.S. 589 (1978) and by the Israeli Supreme Court in *Association for Civil Rights v Minister of Justice*, 5917/97 (2009).

Both the duty of government to make the law known and the right to inspect and to copy judicial records were substantially transformed with the implementation of e-government systems. Such systems present a unique problem in knowledge management. How are rules that are embedded in e-government systems by administrators and programmers to be regulated and to be shared with the public at large?

The issue was presented by Lessig (2000) as a legal theory - "Code is Law". Lessig developed his theory by focusing on cyber platforms, which are used for sharing knowledge, particularly music and other copyright-protected materials. Lessig argued that cyber platforms effectively established new rules, which were not enacted through any democratic process. Such rules might pose "a threat to liberty" and to constitutional principles such as the right to privacy, freedom of speech and access to knowledge. Lessig argued that such rules should be recognized and regulated.

E-government systems are a critical subset of cyber platforms. In implementing e-government systems by various branches of government, from the tax authority through the prison service (Zernik, 2010) to the courts (Zernik, 2010), rules are embedded in computer codes, which are often invisible to the public, and may or may not comply with provisions of the published law. Therefore, sharing knowledge regarding rules, which are embedded in e-government systems, is critical for the duty of government to make the law known, the rule of law and human rights from liberty to the right to own property. Sharing the knowledge regarding such rules is critical for public scrutiny of the conduct of government and protection of human rights.

1 The author represented the NGO in court actions outlined in this report.

Instant case study presents the issue by describing recent Israeli court cases and Israeli Supreme Court judgments, pertaining to the rules that are embedded in e-government system of the Tax Authority, which is used for calculating tax liability, and e-government system of the Administration of Courts, which is used for valid signing, entry and publishing court judgments.

2. The Har Shemesh Affair

In *Har Shemesh v Israeli Tax Authority,* 65/22 (2022) in the Israeli Supreme Court, Appellant Har Shemesh sought to discover the rules, which were embedded in the Tax Authority e-government system ["SHA'AM"], which were used in calculating his tax liability. The Tax Authority denied his requests to provide such information pursuant to Freedom of Information Act ["FOIA"] requests, and the lower court denied his FOIA petition. Therefore, the case was critical for the right to own property and to prevent arbitrary and capricious actions by government against private property.

First, Har Shemesh asked to obtain the algorithm, on which the calculation of his tax liability was based. The Tax Authority responded that that the relevant law and regulations were implemented into the its e-government system without being drafted first as human language specifications, assertions or formulas.

Next, Har Shemesh asked to obtain the actual code of the system. The Tax Authority denied such request, claiming that the code was protected as proprietary information.

In the next round, Har Shemesh claimed that given the significance of the information, the Tax Authority should undertake "reverse engineering" and extract the specification/formulas which were embedded in the system. The Tax Authority denied that request as well, claiming that such efforts required unreasonable allocation of resources.

The lower court denied the Har Shemesh FOIA petition in its first judgment in this affair [Judgment in *Har Shemesh v Tax Authority*, 2663-05-19, (Sept 5, 2019) in the Jerusalem District Court]. Har Shemesh appealed to the Supreme Court, and the Supreme Court granted Har Shemesh's first appeal and overturned the first judgment, sending the case back to the lower court [*Har Shemesh v Tax Authority*, 6782/19, (Dec 24, 2020) in the Supreme Court]. However, in its second judgment in this affair, the lower court defied the Supreme Court and again denied Har Shemesh's petition [Judgment in *Har Shemesh v Tax Authority,* 2663-05-19, (Nov 29, 2021) in the Jerusalem District Court].

In Har Shemesh's second appeal, the Israeli Supreme Court ruled that Har Shemesh could file a new "focused" FOIA request with the Tax Authority, and that the Tax Authority should respond within 60 days after receiving the new FOIA request [*Har Shemesh v Tax Authority*, 65/22 (Feb 8, 2023) in the Supreme Court]. However, it is doubted that the second Supreme Court judgment will end the Har Shemesh affair, which started around 2015.

The Tax Authority appears adamant to avoid sharing the knowledge pertaining to the rules, which are embedded in its e-government system, pertaining to the calculation of Har Shemesh's tax liability.

3. The Human Rights Alert Affair

In *Human Rights Alert NGO v Director of the Courts* (3763/22) in the Supreme Court Appellant Human Rights Alert sought to discover the rules, which were embedded in Net-HaMishpat (case mangement system of the Israeli courts), which provided the manner in which valid and effectual criminal verdicts and sentences were signed and entered in electronic court files. The information, sharing of which was sought, was critical for the right for due process and for liberty itself – indeed to the Rule of Law.

The Administration of the Courts denied FOIA requests to provide such information, claiming that providing any of the information that was requested would undermined the system's "information security" and would cause "close to certain disruption in operation of the system."

The lower court denied Human Rights Alert's FOIA petition [Judgment in Human Rights Alert v Director of the Courts, 56030-02-22 (Apr 14, 2022) in the Jerusalem District Court]. The lower court's judgment was based on its two judgments in the Har Shemesh affair, although the lower court's first judgment in the Har Shemesh affair had already been overturned, and the lower court's second judgment in the Har Shemesh affair was then pending appeal in the Supreme Court

Human Rights Alert arguments in the Supreme Court were in part based on Lessig's (2000) "Code is Law" theory, claiming that the information, which was the rules that were embedded in Net-HaMishpat amounted

to laws or regulations, which had to be published and could not be hidden from the public. Appellant further argued that such rules in fact replaced *Rules of Court* (1936), promulgated during the British Mandate for Palestine, which regulated the work of the Office of the Clerk and the maintenance of paper court files. The *Rules of Courts* were abolished in 2004 in conjunction with development of Net-HaMishpat, and replaced with the *Regulations of the Courts – Office of the Clerk* (2004). However, the rules, which were embedded in Net-HaMishpat system, pertaining to the maintenance of electronic court file, remained hidden.

The same 3-justice panel of Israeli Supreme Court, which heard the Har Shemesh appeal, also heard the Human Rights Alert appeal, in the same seating. During the Supreme Court hearing, Justice Uzi Vogelman stated: "The information, which Sir is seeking, does not exist" [Hearing Protocol in *Human Rights Alert NGO v Director of the Courts,* 3763/22 (Feb 8, 2023) in the Supreme Court]. Appellant argued that such reasoning was inaccurate. The Administration of Courts had indeed claimed that there were no user's manuals for Net-HaMishpat. However, relative to the relevant specifications information the Administration of Courts denied the FOIA request by claiming "information security" concerns.

Furthermore, Appellant argued that claiming that no information existed was clearly unreasonable. For example, the system surely had user's menus, which in themselves reflected some of the rules, relative to operations which were permitted for the users - the judges (Lessing, 2000). Screen shots of Net-HaMishpat menus could be easily produced and provided to Appellant.

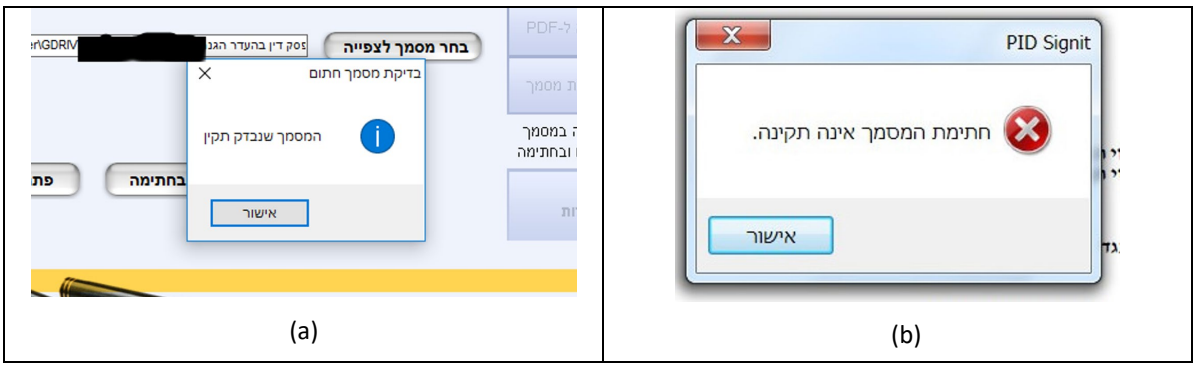
In contrast with the panel's judgment in the Har Shemesh affair, which recognized Har Shemesh's right to obtain at least some of the information from the Tax Authority e-government system, the Human Rights Alert appeal was flatly denied: "After reviewing the arguments of the parties in the appeal, we have found no cause for intervening, and the appeal is denied". However, the Supreme Court panel added an interesting cautionary statement: "...our judgment does not constitute a decision on the issue whether software or IT system code constitutes "information" pursuant to the Freedom of Information Act" [Judgment in *Human Rights Alert NGO v Director of the Courts*, 3763/22 (Feb 8, 2023) in the Israeli Supreme Court]. In the hearing itself, one of justices stated that such question "is not ripe for review and decision."

4. E-signatures in Net-HaMishpat

Article 182 to the Israeli *Criminal Court Procedure Law* (1982) provides: "The Court shall read the verdict and its reasoning in public, sign it and inscribe it with the date of its reading" [underline added – jz].

Until early 2010, when the courts were administered in paper files, the valid signatures appeared on the originals of court decisions as "wet" hand signatures of the judges (see *Figure 2(a)*). The public could inspect and review the judges' signature as part of the right to inspect court records.

In contrast, the visible signatures that today appear on judicial records in Net-HaMishpat are "cut and paste" "graphic signatures", which hold no validity. Administration of the Courts Word Procedure 114/10 clarifies that only the judges' electronic signatures pursuant to the *Electronic Signature Law* (2001) are the valid signatures on judicial records. However, the judges' electronic signatures are information that is not shared – they are inaccessible for review by the public. Judges' electronic signatures can be accessed only when judicial records are electronically served by the court, using dedicated software (*Figure 1*).



(a) (b)

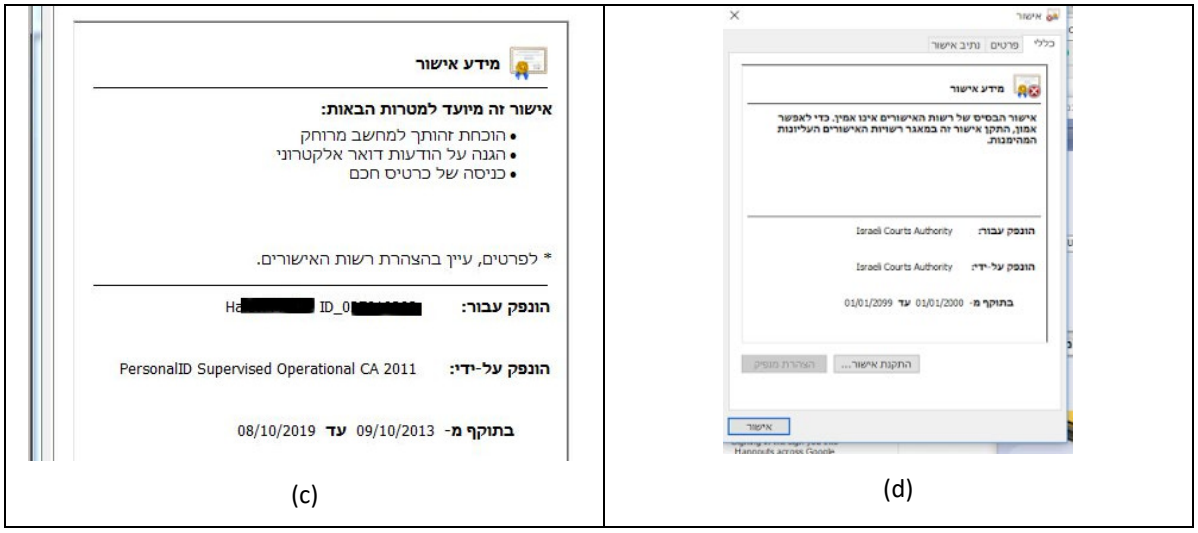


Figure 1: Comparison of Signature Data on a Court Record, which was Filed by an Attorney, and a Judicial Record in Net HaMishpat, using the Dedicated Software of the Israel Bar Association

(a) Inspection of the electronic signature on a court record, which was filed by an attorney: "The document is valid." (b) Inspection of the electronic signature on a judicial record: "The signature of this document is invalid." (c) Signature information of a pleading by an attorney: The signer of the record is identified by name and attorney's license number or ID number, the Certifying Authority is PersonalID corporation, which is registered by the Israeli Registrar of Certifying Authorities pursuant to the *Electronic Signature Act* (2001), and validity of the signing instrument is limited to 6 years. (d) Signature information of a judicial record: "The certification of the signer is invalid"… The purported signer is Israeli Courts Authority, which is also the purported Certifying Authority, and the signature instrument is valid for 100 years…

Comparison of the signature data in Net-HaMishpat of a record filed by an attorney and a judicial record, using the dedicated software of the Israel Bar Association, shows:

- (a) In both cases, the dedicated software fails to indicate the date and time of the signatures.
- (b) Relative to attorneys' signatures, the software shows - "The document is valid." All judges' signatures show - "The signature of this document is invalid."
- (c) Attorneys' signatures identify the signer by name and license number or ID number. All judges' signatures show the signer as "Israeli Courts Authority."
- (d) Attorneys' signatures are certified by PersonalID or Comsign LTD – the two Certifying Authorities that are lawfully registered with the Registrar of Certifying Authorities pursuant to the *Electronic Signature Act* (2001). In contrast, all judges' signatures are certified by "Israeli Courts Authority."

What is "Israeli Courts Authority"?

The question was addressed in separate FOIA requests and FOIA petitions in the courts [*Human Rights Alert v Director of the Courts,* 11963-09-21 and 39537-05-20, in the Jerusalem District Court], at the end of which it was established that there was no lawful government entity named "Israeli Courts Authority," it was merely a "nickname" [Paragraph 1 to Judgment in *Human Rights Alert v Director of the Courts,* 11963-09-21 (Oct 7, 2021) in the Jerusalem District Court].

The conclusion is that the judges' signatures in Net-HaMishpat fail to uphold the two fundamental requirements for validity of an electronic signature: (a) unambiguously identifying the signer, and (b) verifying that the signed document has not been altered after the date of its signing (Weisman, 2001). It should be noted that the issue of user's identification and certification of user's identification (or leaving the identity ambiguous) are among the basic rules, which are embedded in computer codes of cyber platforms, according to the "Code is Law" theory (Lessig, 2000).

Under such circumstances, the mechanism, which was implemented in Net-HaMishpat does not prevent judges from altering a signed document after the date, which appears on its face as the signing date, and there is no simple way for any person, inspecting a judicial record, to ascertain the identity of the signer, the date of the signature, or validity of information, which is shared by the courts as a judicial record.

It should be noted that the electronic signatures in Net-HaMishpat were implemented as "detached electronic signatures." Therefore, the public at large and parties to court case have no simple way to inspect the electronic signatures. The only time that electronic signatures can be inspected is when a judicial record is electronically served by the court. However, as noted above, the Israel Bar Association's dedicated software for inspection of the electronic signatures fails to display the date of the signature. Regardless, the actual date and time of the signature can be retrieved by using an XML reader on the electronic signature file. Using XML reader on judicial records shows that the purported judges' electronic signatures are in fact automatically generated by the system only when the judicial records are served, even when the service is executed years after the date, which is stated on the face of the judicial record as the date of its signature.

Moreover, it is evident that even in judicial records, which were purportedly signed by a panel of 3 judges, there is only one electronic signature, by the fictitious "Israeli Courts Authority."

5. Singing and Entry of a Criminal Verdict – the Roman Zadorov Affair

Roman Zadorov, a Ukrainian citizen, was convicted in September 2010 in the atrocious murder of a 13 year old girl, Tair Rada, and sentenced to life in prison. After Zadorov's appeal in the Israeli Supreme Court in 2014, Prof Mordechai Kremnitzer, one of Israel's leading criminal law experts (who drafted parts of the revision of the Israeli *Penal Law* (1977)) stated: "Conduct of the State Prosecution in the Zadorov file is scary… when you add to it the stance of the Supreme Court and conduct of the Attorney General in recent years, we are left with a justice system that is primarily defensing itself" (Hovel and Linder, 2014). Other criminal law experts and crime investigators also sharply criticized Zadorov's conviction. More than 200,000 Israelis joined social network groups, where the evidence was reviewed in detail, and called for a true police investigation and repeat trial. Finally, in 2023, Zadorov was acquitted after he was granted a second trial.

The 2010 Verdict of the Nazareth District Court file in the Nazareth District Court fails to appear in Net-HaMishpat public access system. It was entered neither in the Decision tab nor in the Judgments tab.

Regulation 2(b) of the *Regulations of Inspection* (2003) provides: "Any person is permitted to inspect judicial decisions that are not lawfully prohibited for publication." Request to inspect the verdict were filed by Human Rights Alert already in 2015. Presiding Judge of the Nazareth District Court Avraham Avraham denied a request to inspect the Verdict in a decision stating [Decision in *State of Israel v Roman Zadorov,* 502/07 (Jan 24, 2016) in the Nazareth District Court]:

> *Requester repeats his requests, which are, allegedly, inspection of judicial records. However, such are not requests to inspect, but an investigation by Requester pertaining to validity of Net-HaMishpat system and an array of arguments relative to conduct of the judicial panel in instant court file. In such matters this Court shall not engage...*

Following the appointment of a new judicial panel for the repeat trial, Human Rights Alert again filed a request to inspect the 2010 Verdict and the corresponding electronic signature. Judge Asher Kula granted the request (Decision in *State of Israel v Roman Zadorov*, 502/07 (June 15, 2022) in the Nazareth District Court]. As a result, the 2010 Verdict was electronically served on Requester. The record appeared invalid and perverted.

Based on all data, which are available to date, the picture that emerges, relative to the September 14, 2010 Verdict, is that on or about September 14, 2010, the Verdict document was generated in the Court's old IT system (*Figure 2(b)*), although at that time, such system was no longer the Court's valid IT system. By September 14, 2010, Net-HaMishpat was already the Court's valid IT system, and the court was administered in electronic files and electronic records.

The old IT system was intended for generating paper judicial record, to be signed using "wet" hand signatures of the judges. However, no copy of the Verdict from the old IT system has been discovered, bearing hand signatures of the judges. An unsigned copy of the Verdict from the old system was discovered as Attachment A to the October 28, 2010 Notice of Appeal, which was filed in the Israeli Supreme Court. Therefore, it is evident that Zadorov's counsel also held at the time an unsigned copy of the September 14, 2010 Verdict (Inspection pursuant to request by Human Rights in *Roman Zadorov v State of Israel,* 7939/10 (March 23, 2015) in the Supreme Court].

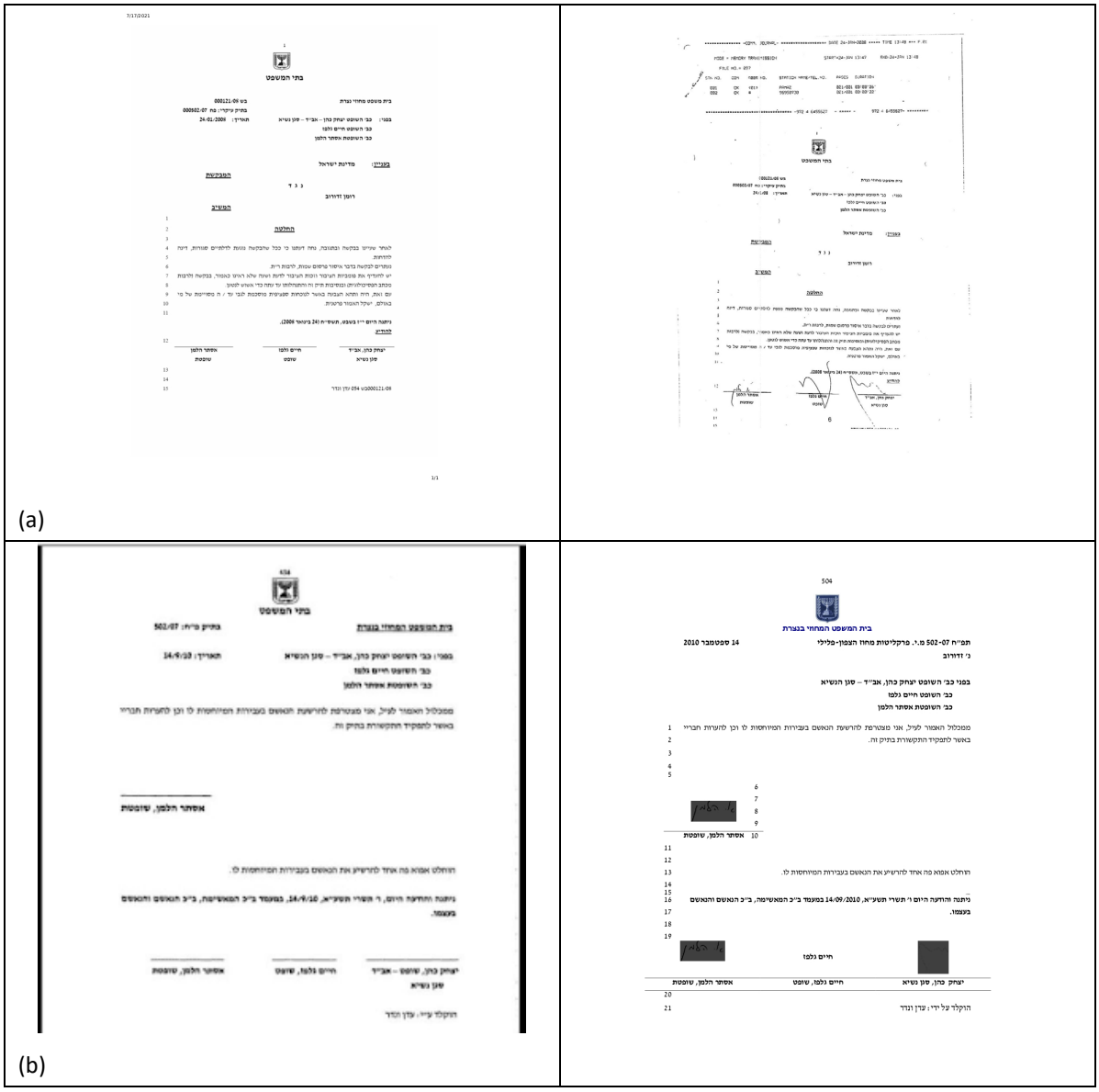


Figure 2: January 24, 2008 Decision and September 14, 2010 Verdict in *State of Israel v Roman Zadorov,* 502/07 in the Nazareth District Court: (a) January 24, 2008 Decision in *State of Israel v Roman Zadorov,* 502/07, while the court was administered in paper court files, prior to the implementation of Net-HaMishpat: Left **– the decision as generated and maintained in the Nazareth District Court's old IT system.** Right **– the decision as it was maintained in the paper court file, and as it was served on the State Prosecution, showing the "wet" hand signatures of the three panel judges [State of Israel response in *Human Rights Alert v Roman Zadorov and State of Israel,* 5501/21 (Nov 29, 2021) in the Supreme Court]. (b)** Left **- the signature page of the September 14, 2010 Verdict, as it appeared in the Nazareth District Court's old IT system.** Right **- as maintained today in Net-HaMishpat**

Prior to the implementation of Net-HaMishpat (in early 2010), the Nazareth District Court was administered in paper court files. Paper decisions and judgments were generated in the Court's old IT system, then printed out and signed using "wet" hand signatures of the judges, and maintained in paper court files (**Figure 2 (a)**).

The Verdict, which is today maintained in Net-HaMishpat was apparently generated at an unknown later date, through a perverted process, as a derivative of the Verdict document from the old IT system (**Figure 2(c)**). For example, the Verdict in Net-HaMishpat bears the page numbers at the head of the page, above the coat of arms of the State of Israel, as was the format in the old IT system, and not in the lower margins, as is the format in Net-HaMishpat. Additionally, the Verdict in Net-HaMishpat shows the "graphic signatures" of only 2

of the three panel judges, and those too appear in the negative form (white on black). Such phenomenon has never been discovered in any other judicial record in Net-HaMishpat.

Furthermore, following Judge Kula's decision, which granted the request to inspect, several old decisions from *State of Israel v Roman Zadorov* (502/07) were served on Requester. The electronic signature files of these judicial records were inspected using an XML reader. It was discovered that the electronic signature files of judicial records, which were over 10 years old, were all generated only on the date of service – July 12, 2022. For example, the data in the electronic signature file of the September 14, 2010 Verdict show that the September 14, 2010 Verdict's electronic signature was generated only on July 12, 2022:

<DocumentCreationDate xmlns="">

2022-07-12T17:53:44.423+03:00

</DocumentCreationDate>

The plausible explanation for such finding is that the signed decision records are generated by Net-HaMishpat only ad hoc – at the time of their service.

Given the dubious validity of the September 14, 2010 Verdict, which was served on July 12, 2022, Human Rights Alert filed a request with the Chief Clerk of the Nazareth District Court to provide a copy of the September 14, 2010 Verdict, certified "True Copy of the Original."

Regardless of repeat requests, the Chief Clerk failed to respond.

The request for certification, which was addressed to the Chief Clerk was eventually referred to Presiding Judge of the Nazareth Distinct Court, Esther Hellman, who denied with prejudice the request for certification [Decision in *State of Israel v Roman Zadorov ,* 502/07 (Sept 11, 2022) in the Nazareth District Court].

Therefore, the right to distinguish between valid and invalid knowledge - in this case, murder conviction and a life imprisonment verdict - which was shared by the court itself, was denied.

Human Rights Alert appealed Presiding Judge Esther Hellman's decision [*Human Rights Alert v State of Israel,* 7215/22, in the Supreme Court]**.** In the appeal, Human Rights Alert argued that the certification of judicial records by the Chief Clerk is a testimonial, wherein the Chief Clerk operated in her capacity as Prothonotary of the Court (Bentham and Bennett, 1959), that a request for certification falls within the duties and authority of the Chief Clerk, and that the judges had no authority to intervene in the autonomous decision of the Chief Clerk, pertaining to certification of judicial record.

Human Rights Alert asked in the appeal that the Supreme Court mandate that the request for certification be returned to the Chief Clerk of the Nazareth District Court for her decision regarding the request for certification of of Roman Zadorov's September 14, 2010 Verdict.

Before the appeal reached a hearing in the Supreme Court, Respondents in the appeal informed Human Rights Alert that a certified copy of the September 14, 2010 Verdict was ready in the Office of the Clerk of the Nazareth District Court (Figure 3).

The certification that was provided by the Nazareth District Court Chief Clerk to Human Rights Alert appears perverted and invalid or dubious at best *(Figure 3)***.** In the certification stamp itself (Right, in blue), the space that was designated for the date of the certification was left empty, and the date of certification was inscribed by hand in the space that was designated for the Chief Clerk's signature. The Chief Clerk's signature was inscribed on a separate stamp (Left, in blue), which is not the certification stamp.

However, since the Chief Clerk responded on the request for certification, the appeal in the Supreme Court was rendered exhausted, and the appeal was dismissed.

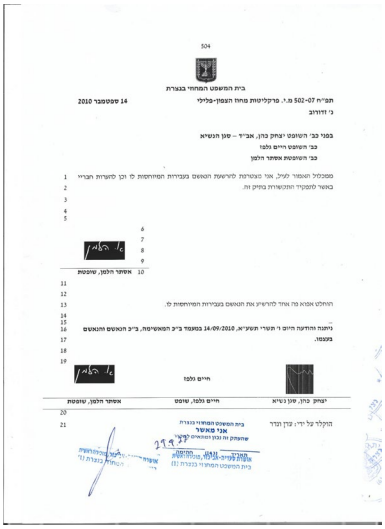


Figure 3: **A copy of the September 14, 2010 Verdict in *State of Israel v Roman Zadorov,* 502/07 (Sept 14, 2010) in the Nazareth District Court – as provided to Appellant Human Rights Alert in *Human Rights Alert v State of Israel,* 7215/22, in the Israeli Supreme Court, in response to a request to obtain the Net-HaMishpat Verdict certified, "True Copy of the Original," by the Chief Clerk of the Nazareth District Court. The certification appears invalid, or dubious at best**

6. Discussion

E-government systems in Israel are usually developed by outsourcing. Therefore, supervising compliance of e-government code with the corresponding law is further complicated. Israeli government decision (1991) prescribed that such systems be developed, validated and implemented pursuant to an elaborate "IT Systems Development and Maintenance Methodology" protocol, which was developed and published by the Israel Accountant General, Ministry of the Finance (2013). The methodology prescribed, *inter alia*, drafting formal specifications prior to signing development contracts and independent inspection and validation of IT systems by state employees before implementing the systems for government service.

Furthermore, procedures of the Accountant General of the Ministry of Treasury prescribed that payment for IT system development and maintenance not be issued , unless documentation was filed of compliance with the Methodology.

However, Israel Government Decision (2014) abolished the requirement for compliance with the methodology. The reasoning was "reducing bureaucratic burden" and promoting the "Digital Israel" project. Therefore, the current state of affairs permits more informal development procedures. Under such circumstances, it is doubted that effective inspection and validation of e-government systems can be performed at all.

The outcome of such informal approach to e-government system development, validation and implementation is clearly demonstrated in the two Israeli Supreme Court cases, outlined in instant report, pertaining to the Tax Authority and the Administration of Courts.

Relative to Net-HaMishpat system of the Administration of Court, Instant report addresses only the issues of signing and entry of criminal judgments. However, Net-HaMishpat is replete with other serious failures in integrity and validity. For example, the Israel State Ombudsman (2022) notes that about 30% of the court files are hidden from public view, including their own existence, mostly with no legal foundation. Entering the court file number of such court files in Net-HaMishpat generates a false and misleading "pop-up message" - "error in court file number." In contrast, the maintenance of a public Index of All Cases is deemed a quintessential requirement in a competent court of record.

Paper administration of government in general and the courts in particular, as well as management and sharing valid information regarding the conduct of government have evolved over centuries, given their preeminent significance for the rule of law. The management and sharing of official public information in a valid manner, which can be distinguished as such by the public at large, was also provided as a constitutional norm already in Article IV, Section 1 to the *U.S. Constitution* (1789):

> *Full Faith and Credit shall be given in each State to the public Acts, Records, and judicial Proceedings of every other State. And the Congress may by general Laws prescribe the Manner in which such Acts, Records and Proceedings shall be proved, and the Effect thereof.*

The office of the Clerk of the Court holds a unique role in managing, sharing and validating court records. It was already provided in the U.S. *Federal Judiciary Act* (1789). Likewise – in England and Australia (Bentham and Bennett, 1959).

Similarly, the British Mandate for Palestine's *Rules of Court* (1936) provided the authority and duty of the Clerk of the Court in the maintenance of court records. In contrast, the Israeli *Regulations of the Court - Office of the Clerk* (2004), which replace the British Mandate's *Rules of Court*, fail to provide the Clerk of the Court, or anybody else, with such authority and duty.

The circumstances pertaining to e-government systems in Israel, documented in instant report, reflect a global trend: The transition from paper administration of government to e-government systems has been implemented with insufficient public oversight. The outcome is loss of fundamental norms, pertaining to the management and sharing of government information in a manner which guarantees the public's ability to ascertain the validity and authenticity of such information.

The proposed solution for the circumstances pertaining to Net-HaMishpat – e-government system of the Israeli courts - includes:

- External, authorized inspection and validation of Net-HaMishpat subject to the joint authority of the Minister of Justice and the Knesset (parliament) Constitution, Law and Justice Committee: The outcome of such review should include defining key failures in the system and methods by which such failures should be corrected and future failures avoided. Such methods may require drafting explicit specifications and their approval by the Minister of Justice and Knesset Constitution, Law and Justice Committee. Furthermore, on site representative of the Minister of Justice with an inspection authority may be required within the technical team of the Administration of Courts, which is charged with maintenance of Net-HaMishpat.
- Amendment of the *Regulations of the Courts – Office of the Clerk* (2004): Regulation 5, which authorized the Director of the Courts to change the regulations at will in e-courts systems should be abolished. Key specifications of Net-HaMishpat should be explicitly promulgated, as well as appointment of Chief Clerks under the authority of the Minister of Justice, and a requirement of periodic reports by the Chief Clerks to the Minister of Justice and Knesset.

The failures, which are outlined in instant report relative to Net-HaMishpat are not unique to Israel. Similar failures have been documented in the past by Human Rights Alert NGO relative to e-government systems in the California and the US federal courts (Zernik, 2010b) and the Los Angeles Sheriff's inmate registration system (Zernik, 2010a). It is likely to be the case in other nations as well.

The 2010 Human Rights Alert submission was in part based on analysis of IT systems of the Superior Court of Los Angeles County and the Los Angeles County Sheriff's Department inmate registration. The submission was incorporated into the final Universal Periodic Review ["UPR"] report of UN Human Rights Commissioner, pertaining to the United States, and summarized as follows (U.N., 2010):

> *45. …HRAlert referred to corruption in the courts and the legal profession, and discrimination of US law enforcement in California.*[70]

The 2015 Human Rights Alert submission was incorporated into the Universal Periodic Review ["UPR"] report of UN Human Rights Commissioner, pertaining to the United States, and summarized as follows (U.N., 2015):

> *57. HRA NGO recommended restoring the integrity of the IT systems of the courts, under accountability to the Congress, with the goal of making such systems as transparent as possible to the public at large.* [193]

The 2018 Human Rights Alert submission was incorporated into the Universal Periodic Review ["UPR"] report of UN Human Rights Commissioner, pertaining to the Israel, and summarized as follows (U.N., 2018):

> *24. HRA-NGO highlighted the serious deterioration in integrity of law and justice agencies as a consequence of the implementation of e-government systems. It affirmed that the validity and integrity of any legal and judicial records of Israel should be deemed dubious at best.*[5]

The transition of government in general, and the courts in particular, from paper administration, which has been developed and established over generations, to e-courts was implemented without sufficient public and elected authorities review and supervision.

The final outcome is fundamental failure in government public knowledge management and sharing – the law and judicial records. Such outcome has generated a clear and present danger to the rule of law and human rights. IT experts should assume a more active role in human rights protection.

References

Bentham R.W. and Bennett, J.M. (1959) "The Office of Prothonotary: Its Historical Development in England and in New South Wales," Sydney Law Review 3 (March 1959).
http://classic.austlii.edu.au/au/journals/SydLawRw/1959/5.pdf

Hovel R. and Linder, R. (2014) "Prof M. Kremnitzer "Conduct of the prosecution in the Zadorov case is scary", [online], *Haaretz*
https://www.haaretz.co.il/magazine/2014-10-16/ty-article/.premium/0000017f-e6b1-dea7-adff-f7fb18ed0000

Israel Accountant General (2013) "IT Systems Development and Maintenance Methodology Version 5.0", [online], Israeli Ministry of the Finance
https://web.archive.org/web/20101211232927/http://ozar.mof.gov.il/hashkal/mol5.htm

Israel Government Decision 1981 (1991)

Israel Government Decision 2097 (2014)
https://www.gov.il/BlobFolder/policy/2097/he/2097.pdf

Israel State Ombudsman (2022) "Administration of Courts: Administration of court processes using Net-HaMishpat", [online], State of Israel Ombudsman.
https://www.mevaker.gov.il/sites/DigitalLibrary/Documents/2022/2022.3/2022.3-304-NET.pdf

Lessig, L. (2000) "Code Is Law, On Liberty in Cyberspace", [online], cartorios.org.
https://cartorios.org/wp-content/uploads/2020/11/LESSIG._Lawrence_Code_is_law.pdf

Messinger, I.S. (2002) "Order in the Courts: A History of the Federal Court Clerk's Office", [online] Federal Judicial Center
https://www.rid.uscourts.gov/sites/rid/files/historical/documents/OrdCourt.pdf

Murphy, E.M. (1982) "The Duty of Government to Make the Law Known", *Fordham Law Review*, Vol 51, p 255.
https://ir.lawnet.fordham.edu/cgi/viewcontent.cgi?article=4606&context=flr

U.N. (2010) Office of the United Nations High Commissioner for Human Rights (2010) "Summary of stakeholders' submissions on the United States : [Universal Periodic Review] : report of the Office of the United Nations High Commissioner for Human Rights" /HRC/WG.6/9/USA/3/Rev.1, [online] United Nations.
https://documents-dds-ny.un.org/doc/UNDOC/GEN/G10/169/65/PDF/G1016965.pdf?OpenElement

U.N. (2015) "Summary of stakeholders' submissions on the United States : [Universal Periodic Review] : report of the Office of the United Nations High Commissioner for Human Rights" HRC/WG.6/22/USA/3, [online], Office of the United Nations High Commissioner for Human Rights.
https://digitallibrary.un.org/record/788753?ln=en

U.N. (2018) "Summary of stakeholders' submissions on Israel : [Universal Periodic Review] : report of the Office of the United Nations High Commissioner for Human Rights" HRC/WG.6/29/ISR/3, [online], Office of the United Nations High Commissioner for Human Rights.
https://digitallibrary.un.org/record/1326596?ln=en

Weisman, R. (2001) "Electronic signature – validity and threats", [Hebrew] *Military and Law,* Vol 15, p 317.

Zernik, J. (2010a) "Data Mining as a Civic Duty – Online Public Prisoners' Registration Systems", *International Journal on Social Media: Monitoring, Measurement, Mining*, Vol 1, pp 84–96.

Zernik, J. (2010b) "Data Mining of Online Judicial Records of the Networked US Federal Courts", *International Journal on Social Media: Monitoring, Measurement, Mining*, Vol 1, pp 69–83.