



Universiteit
Leiden
The Netherlands

The right to break the law? Perfect enforcement of the law using technology impedes the development of legal systems

Custers, B.H.M.

Citation

Custers, B. H. M. (2023). The right to break the law?: Perfect enforcement of the law using technology impedes the development of legal systems. *Ethics And Information Technology*, 25(4). doi:10.1007/s10676-023-09737-3

Version: Publisher's Version

License: [Creative Commons CC BY 4.0 license](https://creativecommons.org/licenses/by/4.0/)

Downloaded from: <https://hdl.handle.net/1887/3716025>

Note: To cite this publication please use the final published version (if applicable).



The Right to Break the Law? Perfect Enforcement of the Law Using Technology Impedes the Development of Legal Systems

Bart Custers¹

Accepted: 7 November 2023
© The Author(s) 2023

Abstract

Technological developments increasingly enable monitoring and steering the behavior of individuals. Enforcement of the law by means of technology can be much more effective and pervasive than enforcement by humans, such as law enforcement officers. However, it can also bypass legislators and courts and minimize any room for civil disobedience. This significantly reduces the options to challenge legal rules. This, in turn, can impede the development of legal systems. In this paper, an analogy is made with evolutionary biology to illustrate that the possibility to deviate from legal rules and existing norms is sometimes necessary for the further development of legal systems. Some room to break the law, for instance, through civil disobedience or imperfect enforcement of the law, will ensure sufficient variation. This allows for properly evolving legal systems that can continue to provide fair solutions, even when society and concepts of fairness further develop.

Keywords Surveillance · Technoregulation · Legal systems · Smart enforcement · Law enforcement · Evolutionary biology · Civil disobedience · Zero-tolerance · Perfect enforcement

Introduction¹

The law is not static. Legal rules and its underlying norms and values continuously change due to developments in society. Every year new laws are adopted in each jurisdiction. For instance, since the EU (or rather its predecessor the European Economic Community – EEC) was established in 1957, it has adopted more than 100,000 legislative acts, with an average of 80 directives, 1200 regulations, and 700 decisions per year (Toshkov, 2014).² In the United States, Congress has enacted more than 30,000 statutes since it was established in 1789, which boils down to approximately

200–400 statutes during each of its biennial terms.³ The number of policies and guidelines established by legislators is even larger. As societies keeps changing, for instance due to new technologies (Wilburn & Wilburn, 2018; Castells, 2020), there is a need for new or supplementary laws and regulations.

The law, or a legal system, can be seen as a model of our society. This model represents the most important values, principles, and rules of our society. This can be seen as a *codification model*, i.e., a model representing the current situation of how we behave. This perspective on the law resembles that of natural scientists, such as physicists, who try to describe the laws of nature in their models as accurately as possible. The laws of nature are unchangeable, whereas the laws of a legal system continuously change, which means that every codification model is in essence a snapshot, but nevertheless a representation (whether accurate or not) of the reality.

Another major difference between law and natural sciences is that legal scholarship is a normative discipline. As a result of this, legal rules are not only a representation of

¹ An earlier version of this article was published in Dutch, see Custers (2022b).

² For detailed statistics, see the EU website at <https://eur-lex.europa.eu/statistics/legislative-acts-statistics.html>.

✉ Bart Custers
b.h.m.custers@law.leidenuniv.nl

¹ eLaw, The Center for Law and Digital Technologies at the Leiden Law School, Leiden University, Leiden, Netherlands

³ See https://en.wikipedia.org/wiki/List_of_United_States_federal_legislation. For detailed statistics, see <https://www.govtrack.us/congress/bills/statistics>.

the current situation, but also an expression of how desirable behavior should look like. This can be seen as a *target model*, i.e., a model representing how we should behave. In each legal system there clearly is a gap between the existing legal rules (the ‘target norms’) and the compliance with these rules. Jaywalking or speeding are typical examples of frequently occurring behavior that is not in compliance with legal rules (Yasin et al., 2021). Enforcement is also often lacking, simply because there is not a police officer on every streetcorner or every mile of highway. For a target model it is important, however, that the gap between the stated norms and the actual compliance and enforcement is not too large. If that would be the case, people may take the rules less seriously, the rules could become less legitimate, and legal certainty would decrease.

The major difference between the two models is that codification models focus on the situation ‘as is’, whereas target models focus on the situation ‘to be’. Hence codification models are mostly descriptive (i.e., describing current norms and values), whereas target models are mostly normative (i.e., putting forward desirable norms and values).

Technology can play an important role in further optimizing and even perfecting enforcement (Mulligan, 2008). Technological developments increasingly enable monitoring and steering the behavior of individuals. An important factor in this is that an increasing share of our communication is online. Cameras, trackers, and sensors can monitor movements, behavior, and statements. We leave everywhere digital traces that may reveal non-compliant behavior. Advanced technologies, such as artificial intelligence (AI), can distil signals from large amounts of data showing who has not perfectly complied with legal rules at some point (Cf. Settanni et al., 2018). Subsequently, law enforcement tools can be employed to further enforce the law.

The technology can also be used to set and enforce rules itself, without any human intervention, via so-called *technoregulation* (Leenes, 2011). In such cases, the technology architecture enforces certain (desirable) behavior and deviations from that norm are physically rendered impossible (Lessig, 2006). Those designing, building, and deploying technology set the rules using technology, which can then be strongly enforced by the way it is designed (so-called technoregulation). A simple example of this in the offline environment is a speed bump, that makes speeding physically impossible without the need to have a law enforcement officer present to fine the offender. The norms that the technology imposes and enforces can be legal norms (e.g., privacy by design) (Hoepman, 2014), but also norms that the designer or manufacturer incorporated into the technology, intentionally or unintentionally (Cf. La Fors et al., 2019). Another example are terms & conditions on a website that can only be accepted by clicking on a checkbox. Here, the

design of the technology prescribes a take-it-or-leave-it scenario. In other words, the technology sets the rules (not the terms & conditions itself, but the rules on consent). These rules cannot be negotiated or challenged by a user (Custers et al., 2018).

Due to these developments, compliance and enforcement can increasingly be optimized and even perfected. Shortages of human enforcers, discussions with offenders, and issues concerning insufficient evidence can all effectively be avoided. Enforcement of the law by means of technology can be much more effective and pervasive than enforcement by humans. However, there is also a downside to this (apart from obvious issues related to privacy and data protection (Solove, 2004) that are beyond the scope of this paper): these developments also lead to less room for civil disobedience and less opportunities to challenge existing legal rules. If the technology itself sets and enforces norms, the legislator is bypassed and, in some cases, also courts and judges are bypassed.

This paper addresses the issue that perfect enforcement of the law using technology can impede the development of legal systems. An analogy is made with evolutionary biology to illustrate that the possibility to deviate from norms is sometimes necessary for the further development of legal systems. Occasionally noncompliance can reveal that current rules are not (or no longer) fair. These signals can easily be missed in the context of perfect enforcement through technology. If there is some room to ‘break the law’, for instance, through civil disobedience or imperfect enforcement of the law, this will ensure sufficient variation and therefore contribute to the proper development of legal systems, i.e., to legal systems that can continue to provide fair solutions, even when society and concepts of fairness further develop.

This paper is structured as follows. Section 2 examines the increasing role of technology in enforcement of the law and how this development enables further optimizing and perfecting the enforcement of the law, via phenomena like surveillance and technoregulation. These developments minimize the possibilities for non-compliance with legal rules. Section 3 discusses why this can lead to issues regarding the development of legal systems, including less ways to challenge existing legal rules, less discretionary power for courts and judges, and less space for proportionality in enforcing the law. Section 4 provides an analogy with evolutionary biology, that puts central the idea that small deviations in the DNA of species cause genetic variations, of which the best fitted will survive. Section 5 draws conclusions and provides suggestions to create some room for breaking the law, for instance, via civil disobedience or imperfect enforcement of the law, because this is necessary for the proper development of legal systems.

Enforcement and regulation using technology

There are two major ways in which technology plays an increasingly important role in enforcing the law: via surveillance and via technoregulation. Surveillance is a well-known phenomenon and extensively discussed in literature (see, for instance, Lyon, 2007; Zuboff, 2019). People leave digital traces everywhere, which means their movements, behavior and statements can be monitored. Since an increasing share of all human interactions and communication is online, there are more and more data available for surveillance. Apart from monitoring communication, also sensors and trackers in mobile phones can be used to monitor or infer locations, transactions and character traits, including needs, preferences, and interests of individuals. Surveillance technologies, when applied ubiquitously, can detect *any* instance of illegal conduct (Rademacher, 2020, p. 248; Rich, 2013, Rademacher, 2019). As soon as the data show that a person did not comply with certain legal rules, enforcement actions can follow (Custers & Stevens, 2021).

Since this concerns large amounts of data, often real-time and in different formats, enforcement by human enforcers immediately causes shortages and capacity problems. Exactly for that reason surveillance technologies and related data analytics technologies are deployed, as these can assist in processing large amounts of data via automated data analyses and extract useful knowledge. This can yield very useful information for human enforcers on how and when to intervene. A straightforward example of this are speed cameras, which generate signals in case of an offence. In many countries, the enforcement processes are completely or almost completely automated: the signals are forwarded to an enforcement agency that subsequently prints a fine that is sent to the offender. Another, more advanced example is cyber agent technology such as chatbots (online artificial chat partners based on AI technology) that can chat with people to determine whether they violated any rules or even predict any non-compliance in the near future (Schermer, 2007).⁴

Although automated analyses can save a lot of work for humans, it often generate high volumes of warning signals ('hits'). For instance, systems for license plate recognition often generate so many signals that human enforcers frequently turn them off, simply because they cannot follow up on all the signals (Koper & Lum, 2019). If police agencies and other law enforcers have insufficient capacity to follow up on all these signals, this can create a sense of urgency among private organizations to act. For instance, if an online platform has the technological capabilities to easily trace

offenders, but competent authorities do not follow up on this, such a platform may decide to take its own measures, such as blocking users or disabling undesirable behavior via the architecture of the online environment – so-called technoregulation. This typically takes when online platforms try to address fake news or hate speech (Kunupudi et al., 2020; Roy et al., 2020).

Technoregulation is the second phenomenon that plays an important role in the enforcement of the law using technology. In technoregulation, it is the technology itself that sets the rules and enforces compliance with these rules, without any intervention of human enforcers. In an offline environment, the architecture of the built environment can enforce certain (desirable) behavior. The speed bumps mentioned before are a typical example of this, but also bus traps, chicanes, and crowd control barriers are typical examples in traffic that disable certain behavior. Other examples in offline environments are fences, walls, and locks that block people from unauthorized access to places. Mosquito high frequency sounds and pink light are typically used to expel loitering youth in some urban areas (Crippen & Klement, 2020; Savoie et al., 2019). The panopticon, i.e., architecture specifically designed to observe people, is another often-mentioned example in this context (Galič et al., 2017).

There are numerous examples of technoregulation in the online environment. A typical example is geofencing, which blocks drones from flying at coordinates close to airports: the software prohibits flying into these areas as if there were invisible walls in the skies (Custers et al., 2015). The online counterparts of fences and locks are cryptography, passwords, and authorizations. Content filtering, computer processing and storage capacity, non-negotiable terms and conditions, and default settings are other examples of how the design of an online environment can guide and steer human behavior in particular directions (Van Loo, 2018).

Technoregulation exists in both private law and public law contexts.⁵ A typical example in private law is an online provider of products and services that unilaterally sets terms and conditions. For instance, social media platforms and search engines unilaterally draft their own terms and conditions, privacy policies and can change them whenever they like, something they often do.⁶ Through the architecture, consumers are confronted with a take-it-or-leave-it situation in which they must accept the entire set of conditions if they want to continue to the next screen. If they disagree, they can opt to refuse the conditions, but that means they will not have access to the service. If the consumer chooses to

⁴ For more on the use of AI in criminal investigations, see Custers (2022a).

⁵ For this reason, in this paper we mostly use the term 'enforcement of the law', rather than 'law enforcement', as the latter focuses on criminal law only.

⁶ Cf. <https://medium.com/@matthewkeys/a-brief-history-of-face-books-ever-changing-privacy-settings-8167dadd3bd0>.

accept the conditions, there is no room for negotiation, for instance, regarding a particularly unfair provision. In case of an old-fashioned contract on paper, some kind of negotiation would have been possible by striking through such a provision, sign the document and submit it. The online architecture, usually presenting a box that must be checked, does not allow for this – which is an example of technoregulation. Another example are the default settings these online service providers use. Default settings are often chosen in ways they best suit the interests of the provider of these services (Kesan & Shah, 2006). Sometimes, the design of the technology offers the possibility to adjust personal settings, e.g., privacy settings, but even then, the options to choose from are determined by the provider of these services (Hansen & Jespersen, 2013; Thaler & Sunstein, 2008).

This raises the question whether such forms of private regulation sufficiently address public interests. These so-called ‘technocontracts’ have implications at a more fundamental level (Bayamlioğlu & Leenes, 2018). In case of regular contracts, disobedient or critical contracting parties can relatively easily ignore some provisions in the contract. That may not be in line with the contractual agreements, but that may not always be relevant and sometimes goes unnoticed. In terms of access to justice it is relevant, however, that actual practices can be discussed and that contract parties can go to court if needed. Interpreting the law and further developing the legal system through jurisprudence are processes that can benefit from disobedient behavior. However, ‘technocontracts’ do not offer any room for this. Non-compliance is no longer an option, simply because the technology does not allow for it any longer. Freedom of choice, disobedient behavior or critique are eliminated in this way (Bayamlioğlu & Leenes, 2018; Leenes, 2011).

Technoregulation is also frequently used in the context of public law. Many of the examples mentioned above relate to traffic, but governments also steer the behavior of citizens via technoregulation in other domains. In many Western countries, the communication between governments and citizens increasingly takes place online. Filing tax returns is still possible on paper in many countries, but in some countries this is increasingly rare. In the Netherlands, for instance, entrepreneurs no longer can file paper tax returns – filing tax returns online is mandatory. Also, administrative appeals against government decisions are increasingly processed online.⁷ When enforcing public order and safety, many governments typically use forms of technoregulation for crowd control (such as static fences and gates, but also dynamic electronic traffic signs, with information based

on camera images and license plate recognition) (Teeuw et al., 2008). Also the abovementioned examples of high frequency sounds and pink light used to expel loitering youth are forms of technoregulation. An online example of technoregulation in criminal law is the obligation in EU member states and the United States that providers of telecommunications services (phone, internet) build their networks in a way that allows interception of communication by law enforcement (Koops et al., 2015, p. 53). This is a design requirement for the technological architecture that tremendously facilitates law enforcement.

In EU data protection law, the use of technoregulation is mandatory, with the underlying aim of protection personal data of data subjects. Article 25 of the EU General Data Protection Regulation (GDPR) prescribes that data controllers should implement technical and organizational measures that are designed to implement data protection principles. This is called data protection by design: the systems should be designed in ways that best protect personal data (Stalla-Bourdillon et al., 2020; Bygrave, 2020). This can be implemented via techniques such as pseudonymization, access controls, encryption, etc. The same article also prescribes that the default settings have to be chosen in such a way that personal data are best protected and personal data can only be processed for the purposes for which the data were originally collected (Borelli & Gatt, 2019).

A typical characteristic of technoregulation is that the technology imposes rules for behavior and that the technology (through its design) enforces these rules itself, without interference of humans (hermand et al., 2018). In all the examples mentioned thus far, behavior that deviates from what the architecture prescribes is impossible. Admittedly, software can be hacked and encryption can be broken, but usually not by the average citizen and it is usually illegal. The norms that technology sets and enforces can be legal norms, but it can also be norms that are incorporated (intentionally or unintentionally) in the technology by the designer or manufacturer.

The combination of these developments allows for the further perfecting of compliance and enforcement of the law. Traditional issues in enforcing the law, such as shortages of human enforcers, discussions with offenders, and issues with insufficient evidence can all effectively be avoided. Less human enforcers are needed when the technologies take over (large parts of) this job. In practice, human enforcers are frequently confronted with offenders that state they were unaware of a certain rule or norm, or that their behavior did not violate any rules or norms. With the use of surveillance technology this can be assessed in detail. More importantly, when technoregulation is deployed, there is no human enforcer to start a discussion anyway. Surveillance usually yields large amounts of data, including relevant

⁷ For instance, in the Netherlands, appeals against traffic fines can be submitted via the Digitaal Loket Verkeer (Digital Traffic Desk), see <https://www.politie.nl/informatie/in-beroep-gaan-tegen-een-verkeersboete.html>.

evidence of non-compliance. In case of technoregulation, evidence is often irrelevant, since enforcement takes place on the spot instead of afterwards – reconstructions, building scenarios, and truth finding are all irrelevant. Since the role of technology in our lives still continues to increase, the number of possibilities for not complying with the rules gradually decreases.

Consequences of these developments

Perfect enforcement of the law using technology significantly reduces the possibilities to challenge legal rules and underlying norms, it may lead to less discretionary power for courts and judges, and less space for proportionality in enforcing the law. These three consequences are discussed below.

Challenging the rules

Some legal rules are not fair. There is a difference between law and ethics. Law sets the (legal) rules we *must* follow, whereas ethics sets the (moral) rules we *should* follow. Take as an example the former Apartheid regime in South Africa. The law prescribed rules that aimed to shape an ethnically segregated society. Regardless of whether this was intended as a codification model or a target model, it was clear the legal system was built on unfair legal rules. There rules were legally valid and were enforced as such, but they certainly were not moral from the perspective of major ethical theories or from the perspective of human rights law. When legal rules are not fair, there is significant inclination to deviate from these rules, particularly among those groups of people who suffer mostly from these rules. Under such conditions, enforcing the law can only be done on a larger scale and at considerably higher costs (Berman, 1991).

The main problem with legal rules that are unethical is that it is hard to challenge them. This played an important role in the South African Apartheid regime or the post WWII racial segregation in the United States: not only are the rules not fair, also the procedures for changing or repealing the rules are unfair. Obviously there are official legislative procedures for changing the rules, mainly via debate in parliament. However, it often takes some amount of civil disobedience or resistance against the existing rules before those who suffer under unfair or unethical legal rules can join the negotiation table and get their issues on the agenda.

When technoregulation is applied, it is even more difficult to challenge the rules than in these historical examples. Although it is usually very clear which norm the technoregulation sets, it is often not clear who imposes that norm and how it can be challenged. In most cases, the

legislator is bypassed and the norms are not established through democratic procedures. For instance, tech companies currently determine which kind of information qualifies as hate speech or fake news and is subsequently filtered and blocked. The criteria for this are not established in a parliamentary debate, not even by the government, but by the companies themselves. Obviously, the fact that rules are made without democratic debate is not an inherent feature of technology. Online platforms are private companies that can impose rules in this way, but this could be changed by the legislator, for instance, by have legal rules on design, functionality, or practices (e.g., rules for misleading practice in consumer law). The point here is that these practices can be hard to challenge, while at the same time our lives increasingly move online, making technology an increasingly important factor in regulating our behavior.

As a result of this, the rules set by technology are gaining importance in regulating our behavior and influencing our choices in comparison to the rules set by lawmakers. The mechanisms challenging architecture are quite different from the mechanisms challenging legal rules, however, rendering the latter mechanisms less effective.

Discretionary power for courts and judges

Legally speaking, it is usually the legislator that plays the main role in the development of legal systems, together with courts and judges. This applies typically to civil law systems such as those in continental Europe. It also applies to common law systems, like in the US or the UK, although the role of case law is more prominent in these systems. Case law usually provides further details and interpretations of existing legal rules, can sometimes lead to new rules, and can occasionally even invalidate certain legal rules. This interplay of relatively abstract legal norms in legislation and the concrete application of these norms in concrete cases by courts and judges usually yields a practical, flexible and manageable legal system. The legislator does not need to establish new rules for each situation and the courts are not bound by rules that are too strict or hard to apply to cases that are slightly different from cases for which the rules were originally intended. In this way, courts and judges can do justice to each case, which obviously goes beyond the mere ‘mechanical’ application of legal rules.

If the discretionary power for courts and judges is considered as an addition to law and regulation, this discretionary power can decrease as a result of technoregulation. Courts and judges will be bypassed more often, since it is the technology itself that sets and enforces the norms. If it is unclear who is behind these norms or how the technology works, it becomes difficult to litigate against this, simply because it is unclear on whose door to knock. Many instances of

technoregulation concern minor adjustments of behavior, which means people are often unaware of this or simply do not care too much about it. It is mostly the combination of instances of technoregulation that may restrict behavior (and thus freedom) of people and therefore can be particularly problematic. As a result of technoregulation, less cases on unfair norms are submitted to courts. If litigation does take place, courts can obviously straighten things out where needed. For instance, courts can judge that a traffic fine for speeding (processed by a speed camera) was unfair after it was explained that next to the driver was his wife, whose waters just broke. Straightening this out requires the intervention of a court, as the speed camera (i.e., technoregulation) does not allow for this.

Although challenging (rules set by) technologies in court is a good mechanism for further development of legal systems, this mechanism is less effective and efficient in highly technological environments. In online architectures, it is often hard to see for people how they are being nudged and manipulated. First, without such awareness, they may not consider challenging this. Second, if they are aware about this, they may not think it is realistic to challenge this (e.g., fighting the system as an individual may be unrealistic and a waste of time). Third, if they really want to challenge the rules set by the online architecture, they may not know how to do this, as it may be unclear whom to address or there may be practical issues addressing those who design, build, and deploy the technology, for instance, because they are located in different jurisdictions.

If laws and regulation are considered as a limitation of the discretionary power for courts and judges, it raises the question whether technoregulation actually can take over this role. Current technologies are not sufficiently sophisticated to make nuanced decisions like courts and judges do, taking into account moral considerations. However, Artificial Intelligence (AI) technology in this area is rapidly becoming more sophisticated. From a technological perspective, the problem is not that judges are not mechanical when applying the law, but rather the assumption that technology is mechanical by definition (Dolin, 2021, p. 9). This is overly simplistic. Nevertheless, the current technologies are still far away from performing the work that courts and judges do. In summary, courts are increasingly bypassed and the technology is unable to fill this gap.

Proportional enforcement

Most legal systems are quite balanced. For instance, criminal law is a balanced system with selective criminal investigation (some crimes are prioritized over others), selective

prosecution (public prosecution services in most countries⁸ can decide whether they prosecute a particular case), different types of sanctions (including imprisonment, fines, probation, parole, community service, mandatory courses for dealing with aggression or addiction, etc.), and maximum penalties that are different for each offence. This means there is some room for non-compliance with legal rules, as long as the behavior is not too excessive. When particular behavior is too problematic, the full apparatus of law enforcement can be put in motion. In summary, criminal law systems are designed in a way that legal rules can be enforced proportionally.

However, this proportionality in enforcement is under pressure in a context in which enforcement of the law heavily relies on technology. Selective criminal investigation and prosecution are partially the result of limited capacity of law enforcement agencies and public prosecution services. Simply because there are not sufficient resources to deal with all the cases, choices have to be made. The size and nature of the issues that law enforcement is confronted with determine how cases are prioritized. With the use of technology, this constraint of scarce capacity largely falls away, creating room for enforcement in cases that were previously not prioritized. As soon as the technology signals that rules are not complied in a particular situation, it becomes harder for law enforcement agencies and public prosecution services to ignore this. At the same time, this raises the question whether this is still proportional.

In other words, it is questionable whether each rule should be enforced in each situation. Research has shown that, on average, people lie several times a day (DePaulo et al., 1996). Obviously, this often concerns trivialities. Jaywalking and speeding are typical examples of offences that many people frequently commit.⁹ For many people it is simply impossible to always, at all times, comply with all rules. Enforcement of all the rules at all times would have significant chilling effects and restrict any sense of freedom. It would not allow people room for making mistakes, which is important for people to learn and develop themselves. As philosopher John Dewey noted, people are not complete, perfect and finished, but rather moving, changing and initiating instead of final (Dewey, 1925, p. 167). People evolve and mature and, for this, people need some room for trying things and, sometimes, need second chances (Cf. Solove, 2007, p. 72–73; Mayer-Schönberger, 2009). The

⁸ This principle of opportunity for public prosecution services exist in France, Germany, the Netherlands, Slovenia, Sweden, and, to some extent, in Belgium and Estonia.

⁹ In 2020 in the Netherlands, there were 7,8 million traffic offences, including speeding, driving though a red light, and handheld phone calls while driving. See <https://www.cjib.nl/nieuws/bijna-78-miljoen-geconstateerde-verkeersovertredingen-2020>.

same actually applies also to legal systems, which also keep evolving, as will be discussed in the next section.

Perfect enforcement of the rules also raises the question which interests are served by such a zero-tolerance approach. Jaywalking is not a terrible shame when it happens in the middle of the night with no-one in sight. It is exactly for this reason that nowadays many traffic lights are turned off during the night at places where there is hardly any traffic. It makes little sense to enforce such norms, simply because the norms have little meaning in such a context. Proportionality requires that the rules are not tightly enforced or even perhaps even disabled. Zero tolerance is simply not appropriate then.

A typical example is the state-wide ban on traffic enforcement cameras in Iowa (Petroski, 2018). Supporters of the ban suggested that the speed cameras were counter to the presumption of innocence and, therefore, not fair. It was argued that speed people should have ‘a sporting chance’ to get away with a specific violation, i.e., a chance to get away with disobedience (Cf. Cheng, 2006). It seems that public support for the cameras was limited because it restricted people’s freedom.

To avoid any misunderstanding: this is not to say that strong enforcement or more enforcement is a bad thing. It is just that perfect enforcement though technology, without human intervention, puts forward a risk, namely that signals are missed that rules are not (or no longer) fair. Here keeping a human in the loop is important. Hence, perhaps breaking particular rules in particular circumstances should be tolerated by not enforcing compliance with these rules. Admittedly, such non-enforcement would offer limited legal certainty, but it would offer room for proportionality. Legal systems that do not always and at all times enforce the rules do still offer the government the possibility to intervene when things get out of hand – with force, if needed. This also works the other way around: since technology can be used to enforce all kinds of norms, it can also be used to enforce norms that are usually less important but incidentally lead to problems. Abolishing such rules would be disproportionate for such rules, whereas selective enforcement could be more proportionate.

Evolution: variation and selection

When considering these developments, a comparison with evolutionary biology readily comes to mind. In evolutionary biology the concepts of ‘genetic variation’ and ‘natural selection’ play a central role. Genetic variation concerns the differences in genetic material of a species. Although the DNA of each species is essentially the same (e.g., one type of DNA grows a human being, another type of DNA grows

a cat), there are also small (smaller) variations within the DNA of each species. As a result of variations in human DNA, not every human being is the same. That can easily be observed in external characteristics, such as body length, skin color, hair color, etc. Genetic variation is the result of sexual reproduction, when the genetic materials of parents is combined, but it will never result in ‘new’ characteristics (i.e., phenotypes) that no human being has (such as blue hair or gills). Apart from sexual reproduction, genetic variation can also be the result of mutations (Futuyma & Kirkpatrick, 2017). If DNA is exposed to radiation or chemicals, it can get damaged or altered. After sexual reproduction, these mutations can introduce new characteristics in a species. These are not really major changes, such as the above-mentioned blue hair or gills, but it does provide for new possibilities.

Not all new variations are beneficial for a species. Some characteristics will prove useful for survival, but others may not. An antelope with longer legs will probably be able to run faster and thus better escape from predators. For similar reasons, other animals have through evolution developed camouflage, stings, and fangs for better survival rates. If a particular variation in DNA yields characteristics that decrease survival rates, then the animal is less likely to sexually reproduce itself and pass along its DNA to the next generation. Variations in DNA that yield characteristics that enable an animal to better adapt to its environment will increase the probability that the animal can sexually reproduce itself (and thus pass along its DNA to the next generation). This is called natural selection (Darwin, 1859).¹⁰ The phenomenon that the animals best adapted to their environment are systematically favored in reproduction is also known as *survival of the fittest*.¹¹ Together, the processes of genetic variation and natural selection yield a gradual change in populations over different generations. In biology, this process of change is called evolution (Futuyma & Kirkpatrick, 2017).

A legal system can also be considered as a gradually changing (evolving) system (Deakin, 2015). From this perspective, consider genetic variation and natural selection. Natural selection is analogous to the process described above, in which particular legal rules are at some point

¹⁰ Darwin introduced the term natural selection, but not the term genetic variation, obviously, because the DNA was only discovered in 1953 by Watson and Crick (Watson & Crick, 1953).

¹¹ The term *survival of the fittest* refers to survival of those who are best fitted (i.e., adjusted, adapted), not to those who are most fit (i.e., health, vitality, endurance). Health, strength and condition contribute to survival for several species, but other species more rely on camouflage or defense strategies for survival. The term survival of the fittest was not introduced by Darwin, but by Herbert Spencer, who drew parallels between economic theories and Darwin’s evolution theory (Spencer, 1864).

no longer used or enforced, or even abolished altogether. A typical example are blasphemy laws, criminalizing contempt, disrespect or lack of reverences concerning deities, sacred objects or religious traditions. Historically, many western countries had criminal law provisions criminalizing blasphemy, but in the 1970s and 80s, these laws were no longer enforced. They were simply not prioritized in criminal investigation and prosecution. Many of these countries (including Australia, Canada, Denmark, France, Greece, Iceland, Ireland, Malta, the Netherlands, New Zealand, Norway, and Sweden) have actually repealed these laws. This shows how legal systems change over time and some rules simply do not survive, because they become outdated. According to some estimates, the average lifespan of written constitutions is approximately 17 years (Ginsburg et al., 2009). Typically, in the Netherlands, on average, existing laws are modified every five years (Jong, 2004). The life expectancy of (abolished) legislation is approximately 25 years (Jong, 2004).

The analogy of genetic variation in legal systems is the possibility of deviating from existing legal rules (cf. beyond existing phenotypes). Ensuring that enforcement of the law is not perfect through the use of technology will provide room for variation. Imperfect enforcement, non-enforcement, civil disobedience, limited capacity for criminal investigation, proportionality in enforcement, and discretionary powers for courts and judges are all mechanisms that can lead to mutations in the system. This ensures variation and a perspective on changes where they may be needed or desirable.

In evolutionary biology, it is generally accepted that species with larger genetic variation have better survival rates (e.g., Booy et al., 2000). Applied to legal systems, survival rates can be seen in terms of public support or legitimacy of the legal system. If a legal system no longer offers fair solutions, for instance, because it is outdated, public support will decline, both for the specific legal rules that are considered unfair and for the legal system as a whole. People will perceive the rules as restrictive, compliance will decline, and enforcing the law can only be done on a larger scale and at considerably higher costs. In other words, enforcement of the law may become too effective to be perceived as fair (Rich, 2013; Rademacher, 2019). That is why variation is also needed in legal systems. The variation (neither too much nor too little) that arises from the room to challenge legal rules can contribute to a legal system that continues to best provide fair solutions when society keeps further developing itself and when concepts of fairness evolve.

It is important to note that in evolutionary biology, evolution does not necessarily equal improvement. For instance, species do not always evolve to become bigger, stronger, or faster. The only criterion is survival of the fittest, i.e.,

how well a species can survive under circumstances, which may sometimes result in smaller or slower species (e.g., to capitalize on energy efficiency or camouflage). In biology, that means those best adapted to (new) circumstances will survive. In law, it could mean that the rules that are best adapted to the (existing or changing) norms and values will survive. This does not necessarily offer assessments or criteria to determine what is good or bad. It is for decision-makers like enforcement officers, lawmakers, and judges, to assess on a case-by-case basis what is good or bad, by allowing some deviations. Technology should be designed in a way that allows them to do this. Similarly, the law should be designed to allow them to do this (e.g., judicial discretion allowing judges to further interpret legal rules and even occasionally bypass some legal rules).

Another important remark is that deviations to the rules, just like mutations in biology, are usually *not* a good or positive thing. Survival rates, also in the legal context, may be low. However, it is the *feature* of possible variations that is important here. In a legal context, non-compliance and selective enforcement do not always lead to mutations in the system and neither are mutations always beneficial. It is just that the benefit of deviation (like in evolutionary biology) is that the variation yields different options. In biology, the best fit will survive and through evolution an entire species may survive. In law, deviations offer a choice for those further developing the legal system (e.g., legislators and courts).

Room for variation not only contributes to the development of legal systems. It also contributes to the development of the technologies used for enforcement. These technologies increasingly are self-learning systems (Wolswinkel, 2020; Passchier, 2021; Custers, 2021). These are types of artificial intelligence (AI) that further evolve on the basis of continuous streams of new data that are fed to them. If there is no variation in those data, the evolution of this technology can grind to a halt. In fact, this means that such technology actually gets better from flaws in the data. To illustrate this, take the example of analyzing data generated by speed cameras. Simple algorithms will conclude that a person who is speeding should receive a fine. A self-learning system, however, could discover that although a person is speeding, this takes place en route to the hospital, which means there is perhaps a justification for non-compliance with the speed limits. Or the system could learn to recognize ambulances, for instance, on the basis of the color and shape of the cars, or on the basis of flashing lights and sirens, and filter these signals. AI technologies need these variations to learn the exceptions to the rule.

Conclusions

Obviously legal rules can be challenged in parliament, via democratic procedures. But, in practice, legal rules are also challenged in many other settings, particularly when the law is enforced. Occasionally noncompliance can reveal that current rules are not (or no longer) fair. Via technoregulation the rules are increasingly set and enforced by technology itself, through the way the technology is designed. The increasing role of technology in the enforcement of the law (via phenomena like surveillance and technoregulation) means that the room for civil disobedience and the opportunities for challenging legal rules gradually decrease. As a result, signals that rules are not (or no longer) fair, can more easily be missed. This can impede the development of legal systems in the sense that legal systems become more rigid and less adaptive to developments in society. As a result, a legal system (or at least parts of it) can become outdated and yield solutions that are less fair or outright unfair. That, in turn, can lead to decreased public support and legitimacy of the legal system.

If there is consensus that allowing some room for variation is valuable, this raises the question how this can be achieved. First, offering protection for possibilities for challenging the rules, discretionary powers for courts and judges, and proportionality in enforcement is important. When establishing rules, it is important to avoid overregulation, i.e., too many and too detailed rules. Overregulation clearly leaves less room for maneuver when applying and enforcing the rules. When enforcing the rules, some room for variation can be achieved by having discretionary powers for those applying the rules, such as law enforcement officers and judges. They should have options to deviate from the rules under circumstances. To avoid that things become too subjective and legal certainty is significantly reduced, this could work according to the comply-or-explain principle for enforcement officers. A comply-or-explain approach would put forward a threshold for those enforcement officers deciding whether a deviation from the rules is acceptable. This ensures that compliance is always the starting point. Technology could then actually play a role in registering deviations from the rules to further improve consistency among those applying the rules in specific cases. Essentially, this means that more enforcement is not a bad thing, as long as a human is kept in the loop.

Second, also framing of these mechanisms is important. Mechanisms like imperfect enforcement, non-enforcement, civil disobedience, and limited capacity for criminal investigation, are often framed as a problem, ignoring the added value that these mechanisms may sometimes have. We think these mechanisms must only be framed as a problem when the consequences for society are getting out of hand (see

also Dolin, 2021, p. 19). Even when technology can contribute to better enforcement of the law, its influence on adequate development of the legal system should weigh in on decisions to actually apply such technologies (Mulligan, 2008).

Obviously, this not an argument in favor or a right to break the law. Such a right would be an oxymoron. Protecting the adequate development of legal systems does not need a legal solution like a right to break the law. To avoid any misunderstanding in this respect, even though it is often citizens who may (want to) challenge the rules, it will (have to) be those applying the rules, such as law enforcement officers or judges, who decide on whether to enforce the rules. If people can decide themselves which rules they comply with, having rules is pointless. If there was to be any discussion on a right to break the law, it would have to be a right not to enforce the law for enforcement officers, not a right for citizens. The question mark in this paper's title is mostly intended to put on the table to issue that the practice of striving for perfect enforcement of the law puts the development of legal systems under pressure. To address this, practical solutions like the mechanisms just mentioned are more suitable than legal solutions. Civil disobedience does not need to be a right, it must mainly be an activity for which sometimes enforcement is appropriate and sometimes it clearly and explicitly is not.

Not all rules in a legal system need to weigh equally and therefore, they do not need to be enforced equally strong. In fact, not all legal rules need to be legally binding. Legal philosopher H.L.A. Hart has proposed a *rule of recognition*, i.e., a rule that determines which legal rules are legally binding (Hart, 2012). Such a rule of recognition could provide more clarity for people regarding the room to challenge particular legal rules, offer more legal certainty regarding enforcement of the law, and help prioritize the limited resources available for criminal investigation and prosecution. In essence, it should be a societal choice to identify which legal rules actually require unconditional compliance and which rules should not be subjected to perfect enforcement (Rademacher, 2020, p. 249–250; Harzog et al., 2015).

It could very well be that the practical limitations regarding enforcement of the law soon become a thing of the past. However, perfect enforcement of the law should not be the goal. Apart from human rights related issues, such as privacy and personal data protection, too tight enforcement of the law can impede the development of legal systems. Room for variation, i.e., opportunities to challenge legal rules in practical settings, will contribute to a flexible legal system that continues to offer fair solutions, even when society changes.

Open Access This article is licensed under a Creative Commons Attribution 4.0 International License, which permits use, sharing, adaptation, distribution and reproduction in any medium or format,

as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons licence, and indicate if changes were made. The images or other third party material in this article are included in the article's Creative Commons licence, unless indicated otherwise in a credit line to the material. If material is not included in the article's Creative Commons licence and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder. To view a copy of this licence, visit <http://creativecommons.org/licenses/by/4.0/>.

References

- Bayamlioglu, E., & Leenes, R. (2018). The 'rule of law' implications of data-driven decision-making: A techno-regulatory perspective, *Law, Innovation and Technology*, 10 (2) (2018), p. 295–313.
- Berman, F. (1991). South Africa: A study of Apartheid Law and its enforcement. *Touro Journal of Transnational Law*, 2(1), 1–66.
- Booy, R., Hendriks, R. J. J., Smulders, M. J. M., Van Groenendaal, J., & Vosman, B. (2000). Genetic Diversity and the Survival of Populations. *Plant Biology* 2: 379–395. 2. <https://doi.org/10.1055/s-2000-5958>.
- Borelli, D., & Gatt, L. (2019). Privacy by design and by default and Data Protection Impact Assessment (DPIA). *European Journal of Privacy Law & Technology*, 100.
- Bygrave, L. A. (2020). Article 25 data protection by design and by default. In L. Bygrave (Ed.), *The EU General Data Protection Regulation (GDPR)*. Oxford University Press.
- Castells, M. (2020). A new society. *The new social theory reader* (pp. 315–324). Routledge.
- Cheng, E. (2006). Structural laws and the puzzle of regulating behavior. *Northwest University School of Law*, 100, 655–718.
- Crippen, M., & Klement, V. (2020). Architectural values, political affordances and selective permeability. *Open Philosophy*, 3(1), 462–477.
- Custers, B., Dechesne, F., Pieters, W., Schermer, B., & van der Hof, S. (2018). Consent and privacy. In A. Müller & P. Schaber (Eds.), *Handbook of the ethics of consent* (pp. 247–258). Routledge.
- Custers, B. H. M. (2022a). AI in criminal law: An overview of AI applications in substantive and procedural criminal law. In B. H. M. Custers, E. Fosch, & Villaronga (Eds.), *Law and artificial intelligence*. Springer.
- Custers, B. H. M. (2022b). Het recht om de wet te overtreden? AI te perfecte rechtshandhaving door technologie kan rechtsonontwikkeling in de weg staan. *Nederlands Juristenblad*, afl. 19, 1532–1539.
- Custers, B. H. M., Oerlemans, J. J., & Vergouw, S. J. (2015). *Het gebruik van drones; een verkennend onderzoek naar onbemande luchtvaartuigen*. Boom Lemma Uitgevers.
- Custers, B. H. M., & Stevens, L. (2021). The Use of Data as evidence in Dutch Criminal courts. *European Journal of Crime Criminal Law and Criminal Justice*, 29(1), 25–46.
- Darwin, C. (1859). *On the origin of species by means of natural selection, or the preservation of favoured races in the struggle for life*. John Murray.
- Deakin, S. (2015). *Law as Evolution, Evolution as Social Order*, Legal Studies Research Paper Series, Working Paper 470, Cambridge: University of Cambridge.
- de Jong, P. O., & Herweijer, M. (2004). Alle regels tellen: de ontwikkeling van het aantal wetten, AMvB's en ministeriële regelingen in Nederland. Den Haag: WODC. <https://www.recht.nl/doc/kst29279-17.pdf>.
- DePaulo, B. M., Kashy, D. A., Kirkendol, S. E., Wyer, M. M., & Epstein, J. A. (1996). Lying in everyday life. *Journal of Personality and Social Psychology*, 70(5), 979–995.
- Dewey, J. (1925). *Experience and nature*. Open Court.
- Dolin, R. (2021). *Technology Issues in Legal Philosophy*, in: Katz, D.M., Dolin, R., Bommarito, M.J. (Eds.) *Legal Informatics*, Cambridge: Cambridge University Press.
- Futuyma, D. J., & Kirkpatrick, M. (2017). *Evolution*, Sunderland, MA: Sinauer Associates.
- Galič, M., Timan, T., & Koops, B. J. (2017). Bentham, Deleuze and beyond: An overview of surveillance theories from the panopticon to participation. *Philosophy & Technology*, 30(1), 9–37.
- Ginsburg, T., Elkins, Z., & Melton, J. (2009). *The Lifespan of Written Constitutions*, Chicago Law School, <https://www.law.uchicago.edu/news/lifespan-written-constitutions>.
- Hansen, P. G., & Jespersen, A. M. (2013). Nudge and the manipulation of choice. *European Journal of Risk Regulation*, 4(1), 3–28.
- Hart, H. L. A. (2012). *The Concept of Law*. Oxford University Press.
- Harzog, W., Conti, G., Nelson, J., & Shay, L. A. (2015). Inefficiently automated law enforcement. *Michigan State Law Review*, p. 1763–1796.
- Hermend, E., Nguyen, T. W., Hosseinzadeh, M., & Garone, E. (2018). Constrained control of UAVs in geofencing applications, Proceedings of the 26th Mediterranean Conference on Control Automation, Zadar, Croatia, June 19–22, 2018, p. 217–222.
- Hoepman, J. H. (2014). Privacy design strategies, in: *IFIP International Information Security Conference*, p. 446–459. Heidelberg: Springer.
- Kesan, J. P., & Shah, R. C. (2006). Setting Software defaults: Perspectives from Law, Computer Science and behavioral economics. *Notre Dame Law Review*, 82(2), 583–634.
- Koops, B. J., Bekkers, R., Bongers, F., Fijnvandraat, M., & See (2015). <https://zoek.officielebekendmakingen.nl/kst-30517-1-b1.pdf>, 53.
- Koper, C. S., & Lum, C. (2019). The impacts of large-scale license plate reader deployment on criminal investigations. *Police Quarterly*, 22(3), 305–329.
- Kunupudi, D., Godbole, S., Kumar, P., & Pai, S. (2020). Toxic language detection using robust filters. *SMU Data Science Review*, 3(2), 12.
- La Fors, K., Custers, B. H. M., & Keymolen, E. (2019). Reassessing values for emerging big data technologies: integrating design-based and application-based approaches, *Ethics and Information Technology*, Volume 21, Number 3, p. 209–226. <https://doi.org/10.1007/s10676-019-09503-4>.
- Leenes, R. (2011). Framing Techno-Regulation: An Exploration of State and Non-State Regulation By Technology, *Legisprudence*, 2011, vol. 5, nr. 2, p. 143–169.
- Lessig, L. (2006). *Code 2.0*. Basic Books.
- Lyon, D. (2007). *Surveillance studies: An overview*. Polity Press.
- Mayer-Schönberger, V. (2009). *Delete: The Virtue of forgetting in the Digital Age*. Princeton University Press.
- Mulligan, C. M. (2008). Perfect Enforcement of Law: When to limit and when to use technology. *Richmond Journal of Law and Technology*, 4(4), 49.
- Passchier, R. (2021). Artificiële intelligentie en de rechtsstaat, Den Haag: Boom Uitgevers.
- Petroski, W. (2018). Iowa Senate OKs ban on traffic enforcement cameras as foes predict more traffic deaths. *Des Moines Register*, <https://eu.desmoinesregister.com/story/news/politics/2018/02/27/traffic-enforcement-cameras-banned-under-bill-passed-iowa-senate/357336002/>.
- Rademacher, T. (2019). Wenn neue technologien alters Recht durchsetzen: Dürfen wir es unmöglich machen, rechtswidrig zu handeln? *JuristenZeitung*, 74, 702–710.
- Rademacher, T. (2020). Artificial Intelligence and Law Enforcement. In T. Wischmeyer, & T. Rademacher (Eds.), *Regulating Artificial Intelligence*. Springer.
- Rich, M. (2013). Should we make crime impossible? *Harvard Journal of Law and Public Policy*, 36, 795–848.

- Roy, P. K., Tripathy, A. K., Das, T. K., & Gao, X. Z. (2020). A framework for hate speech detection using deep convolutional neural network. *Ieee Access : Practical Innovations, Open Solutions*, 8, 204951–204962.
- Savoie, P., Dufresne, M., & Robert, D. (2019). Toward a slow criminology of sociotechnical orderings: A tale of many youth repellents. *Theoretical Criminology*, 23(1), 78–95.
- Schermer, B. W. (2007). *Software agents, surveillance, and the right to privacy: A legislative framework for agent-enabled surveillance*. Leiden University Press.
- Settanni, M., Azucar, D., & Marengo, D. (2018). Predicting individual characteristics from digital traces on social media: A meta-analysis. *Cyberpsychology Behavior and Social Networking*, 21(4), 217–228.
- Solove, D. J. (2004). *The digital person: Technology and privacy in the information age*. New York University Press.
- Solove, J. D. (2007). *The future of reputation*. Yale University Press.
- Spencer, H. (1864). *Principles of Biology*. Williams and Norgate.
- Stalla-Bourdillon, S., Thuermer, G., Walker, J., Carmichael, L., & Simperl, E. (2020). Data protection by design: building the foundations of trustworthy data sharing. *Data & Policy*, 2.
- Teeuw, W. B., Vedder, A. H., Custers, Bart, H. M., Dorbeck-Jung, B. R., Faber, E. C. C., Iacob, S. M., Koops, B. J., Leenes, R. E., de Poot, Henk, J. G., Rip, A., & Vudisa, J. N. (2008). *Security applications for Converging technologies: Impact on the constitutional state and the legal order*. O&B 269.
- Thaler, R. H., & Sunstein, C. R. (2008). *Nudge: Improving decisions about Health, Wealth and Happiness*. Yale University Press.
- Toshkov, D. (2014). *55 years of EU Legislation*, Online presentation, available at: <http://www.dimiter.eu/Eurlex.html>.
- Van Loo, R. (2018). Technology regulation by default: Platforms, privacy, and the CFPB, 2 *Georgia Law and Technology Review*, p. 531–545.
- Watson, J. D., & Crick, F. H. C. (1953). Molecular structure of nucleic acids: A structure for Deoxyribose Nucleic Acid. *Nature*, 171(4256), 737–738.
- Wilburn, K. M., & Wilburn, H. R. (2018). The impact of technology on business and society. *Global Journal of Business Research*, 12(1), 23–39.
- Wolswinkel, C. J. (2020). AR meets AI: een bestuursrechtelijk perspectief op een nieuwe generatie besluitvorming, *Computerrecht*2020/4, p. 22–29.
- Yasin, Y. J., Grivna, M., & Abu-Zidan, F. M. (2021). Global impact of COVID-19 pandemic on road traffic collisions. *World Journal Emerging Surgery*, 16, 51. <https://doi.org/10.1186/s13017-021-00395-8>.
- Zuboff, S. (2019). *The age of surveillance Capitalism: The fight for a human future at the New Frontier of Power*. Profile Books.

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.