



Dieselgate: la crisi della proprietà intellettuale chiusa

Non solo i benchmark dell'elettronica di consumo sono alterati. Ora accade anche in comparti industriali più critici

La pratica scorretta di fare in modo che i prodotti forniscano risultati migliori quando sono sottoposti a benchmark rispetto alle loro prestazioni è molto diffusa nel mondo dell'elettronica di consumo (ne parlammo già nel 2013, sul numero 272 di *PC Professionale*). Ora però la notizia – battezzata “Dieselgate” – che Volkswagen ha modificato i software che controllano le emissioni inquinanti dei motori delle sue automobili per fornire risultati più favorevoli della realtà durante le prove ufficiali cambia radicalmente lo scenario. Perché è la dimostrazione che il virus di questo malcostume non è più limitato alla durata delle batterie o alle prestazioni dell'antenna di un telefono, ma ha infettato comparti industriali ben più critici per la sicurezza dei singoli e della collettività. Senza voler entrare in una dimensione complottista, sarebbe infatti da chiedersi se – in

generale e non in relazione al Dieselgate – a essere truccati o vulnerabili siano solo i software per il controllo delle emissioni o se anche altre parti dei sistemi di controllo delle automobili abbiano subito lo stesso trattamento. Il dubbio sorge se consideriamo che già da almeno un anno Volkswagen e altre ventisei case costruttrici, come rivela il quotidiano inglese *The Independent*, hanno dovuto ammettere che l'antifurto basato sul sistema Megamos Crypto era molto facile da aggirare per via di una debole implementazione della protezione crittografica.

Nel caso del Dieselgate, tuttavia, Volkswagen non è la sola a dover essere sotto accusa. È vero, la casa automobilistica – o meglio, alcuni suoi alti

dirigenti – hanno barato, ma nessuno degli enti di controllo (ministeri dei trasporti, motorizzazioni e via discorrendo), ha mai effettivamente verificato il funzionamento dei software che fanno funzionare un'automobile. In altri termini, i processi di omologazione e controllo sembrano essere basati sul considerare un'autovettura come una “scatola nera”: ad essere verificati sono i risultati dei test, senza entrare nel merito di cosa ci sia, letteralmente, sotto il cofano.

E finalmente veniamo al punto: anche se qualche funzionario pubblico più illuminato avesse pensato di dare un'occhiata ai software e ai firmware, con buona probabilità gli sarebbe stato risposto che questo era impossibile perché i codici sorgenti erano “oggetto di proprietà intellettuale” e la loro messa a disposizione avrebbe potenzialmente danneggiato gli interessi della casa automobilistica.

Scatola nera sigillata

I processi di omologazione e controllo non sembrano essere entrati nel merito del software che fa funzionare l'automobile

Se l'elettronica delle automobili fosse stata gestita da software open source, con buona probabilità lo scandalo Dieselgate non sarebbe mai scoppiato perché la paura di essere più facilmente scoperti avrebbe sconsigliato anche il semplice tentativo di truccare informaticamente i motori. E dunque sarebbero stati evitati danni ad ambiente e cittadini, oltre che miliardi di costi in termini di danni diretti e indiretti al comparto dell'autotrasporto e ai suoi investitori.

Il merito del Dieselgate, dunque, è in primo luogo quello di avere sdoganato il tema dell'open source dall'ambito di nicchia (grande, ma sempre nicchia) della consumer electronic dimostrando

che la questione del (negato) accesso ai codici sorgenti ha delle implicazioni di portata estremamente più ampia e pericolosa per la collettività.

In secondo luogo, il Dieselgate ha dimostrato chiaramente che un certo modo di intendere la proprietà intellettuale – analogamente a quanto accade con una certa “visione” della privacy – è diventato un sistema per nascondere comportamenti illeciti piuttosto che uno strumento per tutelare legittimi interessi industriali e personali.

Non serve una legge per risolvere questo problema. Le direttive comunitarie sulla proprietà intellettuale e industriale già contengono la possibilità di gestire in modo flessibile modi e criteri per accedere liberamente al codice sorgente di un software, tutelando nel contempo la giusta esigenza di segretezza che costituisce un elemento di vantaggio sui concorrenti. E' necessario, piuttosto, che l'industria (non solo) dell'autotrasporto rifletta sull'effettiva utilità di continuare a gestire i propri beni immateriali (software) con la stessa antica logica riservata a pignoni, mozzi e testate.

Parlo di industria nel suo insieme e non di singola casa automobilistica perché anche l'elettronica, come altri componenti, è spesso realizzata da fornitori che operano nel cosiddetto “indotto” e che a loro volta vincolano la realizzazione di software a draconiani accordi basati su una logica proprietaria che lasciano poco spazio al controllo indipendente sul software.

Anche questi fornitori esterni dunque potrebbero essere coinvolti nel Dieselgate? Astrattamente sarebbe possibile. Perlomeno in Italia, infatti, grazie al decreto legislativo 231 del 2001, le aziende che omettono di controllare i propri processi gestionali e produttivi in relazione alla tutela ambientale possono essere sanzionate penalmente insieme ai singoli dirigenti e dipendenti autori materiali dell'atto illecito. Bisognerebbe dunque ripercorrere l'intera filiera produttiva per capire fino a che punto l'accaduto abbia riguardato la sola Volkswagen o se ci siano stati coinvolgimenti di altri soggetti che le ruotavano attorno. •