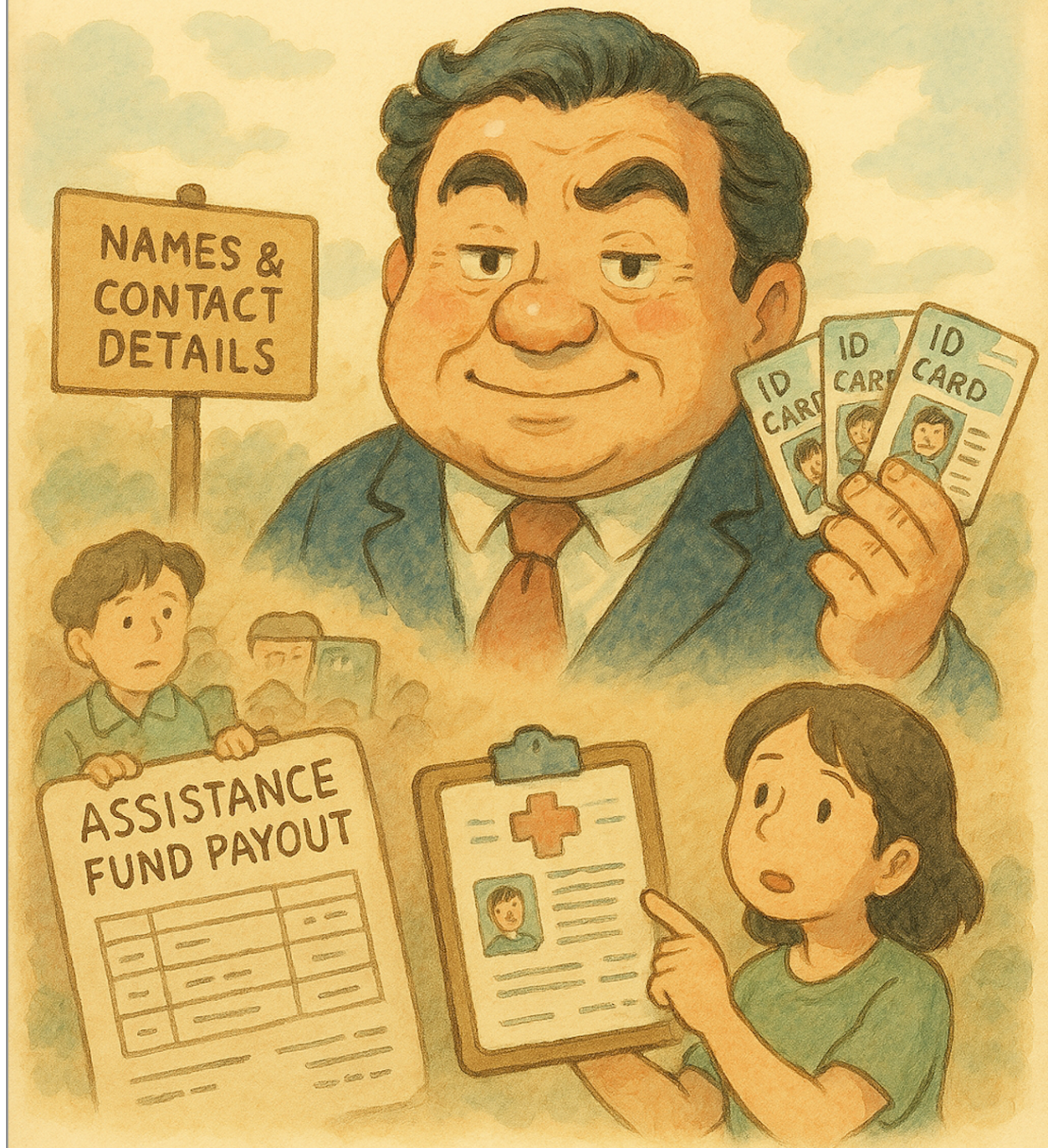


PHILIPPINE ELECTIONS 2025

The Alarming Rise of Unsecured Personal Data Processing



Philippine Elections 2025: The Alarming Rise of Unsecured Personal Data Processing

By R. Milanes, Unpublished

As the Philippine Elections 2025 draw near, the national spotlight once again shines not only on the political promises and platforms of aspiring leaders, but also on the disturbing trend of how personal data is being processed—and exploited—increasingly without regard to privacy, security, or the rule of law.

In an age where data is currency, it is alarming how politicians and public institutions continue to treat sensitive personal information with reckless abandon. From campaign gimmicks disguised as public service initiatives to over-collection of data for aid disbursement, we are witnessing an insidious erosion of our fundamental right to privacy.

✗ The Politicization of Identification Cards

A growing number of politicians are issuing their own localized “identification cards” under the guise of community programs, senior citizen benefits, or youth aid. These IDs, often bearing the politician’s face and logo, collect a full range of personal data—complete names, birth dates, addresses, and even government-issued ID numbers.

What safeguards are in place to protect this information? Who manages the database? Where is the privacy notice? These initiatives are never registered with the National Privacy Commission (NPC), nor do they comply with the Data Privacy Act of 2012. In many cases, the individuals collecting this data are political volunteers with no training in data protection, no accountability, and no idea that they are handling sensitive information unlawfully.

This trend is not only a flagrant violation of data protection principles—it’s a form of digital exploitation, using personal information as a political asset.

📱 Dangerous "Transparency"

In the spirit of “transparency,” some local governments and political figures publicly post lists of scholarship recipients, financial aid beneficiaries, or livelihood grant recipients on social media—complete with full names, middle names, barangay addresses, and contact numbers.

While transparency in public funds is crucial, it must never come at the cost of an individual’s privacy and safety. These lists expose citizens to identity theft, scams, and targeted harassment. In some cases, such posts have been

used to imply political loyalty, weaponizing public assistance as a tool for coercion.

This is not transparency—it is digital doxing, and it must be condemned.

Health Data in Unsafe Hands

There is also a deeply concerning trend of health-related data being processed by untrained individuals under political programs. Medical missions and free check-ups are commendable efforts, but the handling of diagnostic information, medical history, and other sensitive health data by unlicensed personnel or volunteers creates huge risks of data leaks, misdiagnosis, or misuse.

Health data is classified as sensitive personal information under Philippine law. It should be processed with the highest level of security and ethical care—not scribbled on logbooks or left on open spreadsheets for anyone to access.

Over-Collection in Cash Payouts

Assistance funds for calamity relief, livelihood aid, and poverty reduction programs are now often tied to data forms that request far more than what is necessary. From TINs to marital status, educational background to voter registration numbers—these forms often serve as tools for profiling rather than service delivery.

The Data Privacy Act mandates proportionality in data collection: collect only what is necessary, for a clearly defined and lawful purpose. Yet during elections, many of these data gathering efforts are framed as "requirements" for aid, exploiting the vulnerable and reinforcing digital patronage.

The advocates of data protection must raise their voices louder than ever. Citizens must be empowered to ask questions:

- **Why is this data being collected?**
- **Where will it be stored?**
- **Who will access it, and for how long?**
- **Is there a privacy policy?**

It is also time for the **National Privacy Commission**, the **Commission on Elections**, and **civil society organizations** to establish stronger guidelines and monitoring mechanisms to ensure that no candidate or public servant weaponizes personal data in their quest for votes.

The Philippine Elections 2025 must not only be a test of our democratic resolve—but of our ability to protect our people in the digital age.

Because data is not just a string of numbers or names. It is identity. It is dignity. And in the wrong hands, it is power abused.